The President's
IDENTITY THEFT
Task Force Report

September 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
26 SEP 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The President's Identity Theft Task Force Report	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **President's Identity Theft Task Force,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**70**	

Table of Contents

Identity Theft Task Force Members

Michael B. Mukasey, Chairman
Attorney General

William E. Kovacic, Co-Chairman
Chairman, Federal Trade Commission

Henry M. Paulson, Jr.
Department of the Treasury

Carlos M. Gutierrez
Department of Commerce

Michael O. Leavitt
Department of Health and Human Services

James B. Peake
Department of Veterans Affairs

Michael Chertoff
Department of Homeland Security

Jim Nussle
Office of Management and Budget

Alexander Lazaroff
United States Postal Service

Ben S. Bernanke
Federal Reserve System

Michael W. Hager
Office of Personnel Management

Sheila C. Bair
Federal Deposit Insurance Corporation

Christopher Cox
Securities and Exchange Commission

JoAnn Johnson
National Credit Union Administration

Michael J. Astrue
Social Security Administration

John C. Dugan
Office of the Comptroller of the Currency

John M. Reich
Office of Thrift Supervision

Introduction

Two years ago, the President launched a new era in the fight against identity theft by issuing an executive order establishing the Identity Theft Task Force.[1] The executive order charged 15 federal departments and agencies with crafting a comprehensive national strategy to combat more effectively this pernicious crime, which afflicts millions of Americans each year and, in some cases, causes devastating damage to its victims. One year later, on April 11, 2007, the Task Force submitted its Strategic Plan to the President. The Strategic Plan examined the nature and scope of identity theft and offered a far-reaching series of recommendations to reduce its incidence and impact. Although these recommendations were directed primarily at improving the federal government's response to identity theft, the Task Force recognized that everyone—consumers, the private sector, and federal, state, and local governments—has a role to play in fighting this crime.

This report documents the Task Force's efforts to implement the Strategic Plan's recommendations. The Task Force has successfully carried out most of the recommendations or is making substantial progress in doing so.

The Strategic Plan included recommendations in four key areas:

- **Data protection**—keeping consumer data out of the hands of criminals;
- **Avoiding data misuse**—making it harder for criminals to exploit consumer data;
- **Victim assistance**—making it easier for victims to detect and recover from identity theft; and
- **Deterrence**—increasing prosecution and punishment of perpetrators.

In these four areas, the Task Force made a total of 31 recommendations, ranging from small, incremental steps to broad policy changes.

First, with respect to **data protection**, the Task Force has promoted a new culture of security in the public and private sectors. For the public sector, the Task Force member agencies launched a variety of initiatives aimed at making the federal government a better custodian of sensitive personal information. The Office of Management and Budget, for example, worked to educate all federal agencies on improving data security practices and is monitoring their performance in doing so. The Office of Personnel Management led an interagency initiative to eliminate unnecessary uses of Social Security numbers (SSNs)—one of the most valuable commodities for identity thieves—in federal government human resource functions, while individual agencies began to eliminate unnecessary uses of SSNs in other aspects of their work.

The Task Force encouraged similar data security efforts in the private sector by launching several policymaking, outreach, and enforcement initiatives.

The Task Force expanded its data security and identity theft business and consumer education campaigns through speeches, videos, articles, brochures, testimony, interviews, tip sheets, and a best practices workshop for businesses. In one important example, the U.S. Postal Service delivered a mailing in early 2008 to 146 million U.S. residences and businesses with advice on how to protect themselves against identity theft. Task Force member agencies continued to investigate and, where appropriate, take civil, administrative, or criminal enforcement action against individuals and entities for violations of data security laws and regulations.

Second, the Task Force examined ways to prevent identity theft by making it harder for thieves to misuse consumer data. Member agencies held two public workshops that explored means of **improving consumer authentication** processes to prevent thieves from using stolen personal information to access existing accounts or open new ones. One of the workshops specifically addressed the availability and use of SSNs in the authentication process, and whether there are better and less sensitive substitutes. These workshops provided opportunities for public and private sector representatives and consumer advocates to explore these issues.

Third, the Task Force launched a number of initiatives to **assist identity theft victims** when they begin the sometimes arduous task of repairing their credit and restoring their good names. Task Force member agencies over the past year provided identity theft training to over 900 law enforcement officers—often the first sources to whom victims turn—from over 250 agencies. Task Force members also trained victim assistance counselors and provided grants to organizations that directly help identity theft victims. Task Force members developed and posted an Identity Theft Victim Statement of Rights and are working closely with the American Bar Association on a pro bono legal assistance program for identity theft victims. Task Force members also are continuing to evaluate the effectiveness of various laws and programs designed to help victims, such as state identity theft "passport" programs, state credit freeze laws, and rights granted under the Fair and Accurate Credit Transactions Act of 2003.

Fourth, the Task Force worked to improve law enforcement's ability to **investigate, prosecute, and punish** identity thieves by proposing legislation to Congress, improving coordination and training for local law enforcers, and targeting criminal enforcement initiatives. Task Force members also are enhancing international cooperation by partnering with foreign law enforcement agencies in identity theft investigations and providing them with training and assistance, and encouraging greater information sharing among and between law enforcement agencies and the private sector.

The Task Force's Strategic Plan notes that there is no simple solution to identity theft. It is an ever-evolving problem with many dimensions. Public concerns about the security of personal information and identity theft remain at high levels, with potentially serious consequences for the functioning of our economy.[2] The efforts of the Task Force over the past year to implement the Plan's recommendations have underscored the need for a comprehensive and coordinated response from both the public and private sectors. These efforts have already made a difference and will continue to do so in the coming years.

Task Force Recommendations from April 2007 Strategic Plan

IDENTITY THEFT PREVENTION

RECOMMENDATION 1: DECREASE THE UNNECESSARY USE OF SSNs IN THE PUBLIC SECTOR

- Complete Review of Use of SSNs
- Issue Guidance on Appropriate Use of SSNs
- Require Agencies To Review Use of SSNs
- Establish a Clearinghouse for Agency Practices That Minimize Use of SSNs
- Work with State and Local Governments To Review Use of SSNs

RECOMMENDATION 2: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

RECOMMENDATION 3: EDUCATE FEDERAL AGENCIES ON HOW TO PROTECT THEIR DATA AND MONITOR COMPLIANCE WITH EXISTING GUIDANCE

- Develop Concrete Guidance and Best Practices
- Comply with Data Security Guidance
- Protect Portable Data Storage and Communication Devices

RECOMMENDATION 4: ENSURE EFFECTIVE, RISK-BASED RESPONSES TO DATA BREACHES SUFFERED BY FEDERAL AGENCIES

- Issue Data Breach Guidance to Agencies
- Publish a "Routine Use" Allowing Disclosure of Information Following a Breach

RECOMMENDATION 5: ESTABLISH NATIONAL STANDARDS EXTENDING DATA PROTECTION SAFEGUARDS REQUIREMENTS AND BREACH NOTIFICATION REQUIREMENTS

RECOMMENDATION 6: BETTER EDUCATE THE PRIVATE SECTOR ON SAFEGUARDING DATA

- Hold Regional Seminars for Businesses on Safeguarding Information
- Distribute Improved Guidance for Private Industry

RECOMMENDATION 7: INITIATE INVESTIGATIONS OF DATA SECURITY VIOLATIONS

RECOMMENDATION 8: INITIATE A MULTI-YEAR PUBLIC AWARENESS CAMPAIGN

- Develop a Broad Awareness Campaign
- Enlist Outreach Partners
- Increase Outreach to Traditionally Underserved Communities
- Establish "Protect Your Identity Days"

RECOMMENDATION 9: DEVELOP AN ONLINE CLEARINGHOUSE FOR CURRENT EDUCATIONAL RESOURCES

RECOMMENDATION 10: HOLD WORKSHOP ON AUTHENTICATION

RECOMMENDATION 11: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

VICTIM ASSISTANCE AND RECOVERY

RECOMMENDATION 12: PROVIDE SPECIALIZED TRAINING ABOUT VICTIM RECOVERY TO FIRST RESPONDERS AND OTHERS PROVIDING DIRECT ASSISTANCE TO IDENTITY THEFT VICTIMS

- Train Local Law Enforcement Officers
- Provide Educational Materials for First Responders That Can Be Readily Used as a Reference Guide for Identity Theft Victims
- Distribute an Identity Theft Victim Statement of Rights
- Develop Nationwide Training for Victim Assistance Counselors

RECOMMENDATION 13: DEVELOP AVENUES FOR INDIVIDUALIZED ASSISTANCE TO IDENTITY THEFT VICTIMS

- Engage the American Bar Association To Develop a Program Focusing on Assisting Identity Theft Victims with Recovery

RECOMMENDATION 14: AMEND CRIMINAL RESTITUTION STATUTES TO ENSURE THAT VICTIMS RECOVER FOR THE VALUE OF TIME SPENT IN ATTEMPTING TO REMEDIATE THE HARMS THEY SUFFERED

RECOMMENDATION 15: EXPLORE THE DEVELOPMENT OF A NATIONAL PROGRAM ALLOWING IDENTITY THEFT VICTIMS TO OBTAIN AN IDENTIFICATION DOCUMENT FOR AUTHENTICATION PURPOSES

RECOMMENDATION 16: ASSESS EFFICACY OF TOOLS AVAILABLE TO VICTIMS

- Conduct Assessment of FACT Act Remedies Under FCRA
- Conduct Assessment of State Credit Freeze Laws

LAW ENFORCEMENT

RECOMMENDATION 17: ESTABLISH A NATIONAL IDENTITY THEFT LAW ENFORCEMENT CENTER

RECOMMENDATION 18: DEVELOP AND PROMOTE THE ACCEPTANCE OF A UNIVERSAL IDENTITY THEFT REPORT FORM

RECOMMENDATION 19: ENHANCE INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND THE PRIVATE SECTOR

- Enhance Ability of Law Enforcement To Receive Information from Financial Institutions
- Initiate Discussions with the Financial Services Industry on Countermeasures to Identity Thieves
- Initiate Discussions with Credit Reporting Agencies on Preventing Identity Theft

RECOMMENDATION 20: ENCOURAGE OTHER COUNTRIES TO ENACT SUITABLE DOMESTIC LEGISLATION CRIMINALIZING IDENTITY THEFT

RECOMMENDATION 21: FACILITATE INVESTIGATION AND PROSECUTION OF INTERNATIONAL IDENTITY THEFT BY ENCOURAGING OTHER NATIONS TO ACCEDE TO THE CONVENTION ON CYBERCRIME, OR TO ENSURE THAT THEIR LAWS AND PROCEDURES ARE AT LEAST AS COMPREHENSIVE

RECOMMENDATION 22: IDENTIFY COUNTRIES THAT HAVE BECOME SAFE HAVENS FOR PERPETRATORS OF IDENTITY THEFT AND TARGET THEM FOR DIPLOMATIC AND ENFORCEMENT INITIATIVES FORMULATED TO CHANGE THEIR PRACTICES

RECOMMENDATION 23: ENHANCE THE U.S. GOVERNMENT'S ABILITY TO RESPOND TO APPROPRIATE FOREIGN REQUESTS FOR EVIDENCE IN CRIMINAL CASES INVOLVING IDENTITY THEFT

RECOMMENDATION 24: ASSIST, TRAIN, AND SUPPORT FOREIGN LAW ENFORCEMENT

RECOMMENDATION 25: INCREASE PROSECUTION OF IDENTITY THEFT

- Designate an Identity Theft Coordinator for Each U.S. Attorney's Office
- Evaluate Monetary Thresholds for Prosecution
- Encourage State Prosecution of Identity Theft
- Create Working Groups and Task Forces

RECOMMENDATION 26: CONDUCT TARGETED ENFORCEMENT INITIATIVES

- Unfair or Deceptive Means To Make SSNs Available for Sale
- Identity Theft Related to the Health Care System
- Identity Theft by Illegal Aliens

RECOMMENDATION 27: REVIEW CIVIL MONETARY PENALTY PROGRAMS

RECOMMENDATION 28: CLOSE THE GAPS IN FEDERAL CRIMINAL STATUTES USED TO PROSECUTE IDENTITY-THEFT-RELATED OFFENSES TO ENSURE INCREASED FEDERAL PROSECUTION OF THESE CRIMES

RECOMMENDATION 29: ENSURE THAT AN IDENTITY THIEF'S SENTENCE CAN BE ENHANCED WHEN THE CRIMINAL CONDUCT AFFECTS MORE THAN ONE VICTIM

RECOMMENDATION 30: ENHANCE TRAINING FOR LAW ENFORCEMENT OFFICERS AND PROSECUTORS

- Develop Course at the National Advocacy Center Focused Solely on Investigation and Prosecution of Identity Theft
- Increase Number of Regional Identity Theft Seminars
- Increase Resources for Law Enforcement Available on the Internet
- Review Curricula To Enhance Basic and Advanced Training on Identity Theft

RECOMMENDATION 31: ENHANCE THE GATHERING OF STATISTICAL DATA MEASURING THE CRIMINAL JUSTICE SYSTEM'S RESPONSE TO IDENTITY THEFT

- Gather and Analyze Statistically Reliable Data from Identity Theft Victims
- Expand Scope of the National Crime Victimization Survey and Conduct Targeted Surveys
- Review Sentencing Commission Data
- Track Prosecutions of Identity Theft and the Amount of Resources Spent

Implementation of the Strategic Plan

RECOMMENDATION 1: DECREASE THE UNNECESSARY USE OF SSNs IN THE PUBLIC SECTOR

Since its inception, the Task Force has recognized that the public sector, as a collector and custodian of sensitive consumer information, must play a central role in any coordinated plan to address identity theft. The Strategic Plan contains a variety of recommendations regarding public sector data security initiatives. Although many of these initiatives focus on safeguarding data, this first recommendation is aimed at reducing the availability of sensitive data by eliminating the unnecessary use of Social Security numbers (SSNs) in the public sector. The SSN is highly valuable for identity thieves because it is often a necessary (if not necessarily sufficient) item of information that a thief needs to open new accounts in the victim's name. This recommendation reflects a basic tenet of data security: One of the most practical and cost-effective ways to prevent breaches is to collect and maintain sensitive data only when it is necessary to do so.[3]

To assist the government in identifying and eliminating unnecessary SSN uses, the Task Force made the following specific recommendations:

Complete Review of Use of SSNs

The Task Force recommended that the Office of Personnel Management (OPM) take steps to eliminate, restrict, or conceal the use of SSNs in its collection of human resource data from federal agencies and on OPM-based papers and electronic forms. In making this recommendation, the Task Force recognized that OPM, in its oversight of many of the federal government's human resources functions, can play a key role in reducing SSN usage by changing the forms and procedures used by the federal government that have commonly required this identifier.

OPM has developed and begun implementation of a plan to reduce unnecessary uses of SSNs. In spring 2007, OPM offices inventoried their use of SSNs on forms and in information systems. Through the agency's IT Security Working Group, OPM offices are now reviewing these inventories and identifying opportunities for eliminating unnecessary SSN usage. In support of this initiative, OPM's Director has issued reminders to OPM employees and contractors to reduce unnecessary SSN usage and to take appropriate measures to protect all personally identifiable information (PII).

In addition, OPM, in cooperation with other agencies, has been studying the feasibility of creating an alternate identifier for federal employees that would phase out the use of SSNs for all functions except the initial intake of the employee into federal service. At the request of the Identity Theft Task Force, OPM, working with the Social Security Administration (SSA), has developed

a framework entitled the Unique Employee Identifier Concept of Operation (UEID CONOP) to transition federal employees to an alternate identifier. OPM submitted the UEID CONOP to the Task Force on January 31, 2008. At the same time, the Office of Management and Budget (OMB) has been partnering with federal agencies to study alternatives to their use of SSNs in federal programs, and other federal agencies are developing alternative identifiers for their employees.

▶ *Issue Guidance on Appropriate Use of SSNs*

The Task Force recommended that OPM issue guidance on the appropriate and inappropriate use of SSNs in federal employee records. This recommendation was intended to ensure a unified approach to SSN usage by federal agencies. On June 18, 2007, OPM issued "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft" to the Chief Human Capital Officers of all federal departments and agencies.[5] The Guidance has two goals: (1) to eliminate the unnecessary use of SSNs in federal personnel records and (2) to strengthen the protection of employees' sensitive information from theft or loss.

To help agencies meet these goals, the Guidance first describes existing regulatory requirements that govern the handling of personnel records. Next, the Guidance directs agencies to implement additional security measures, including:

- restricting access to SSNs to those whose official duties require such access;
- requiring individuals who have access to SSNs and other sensitive personal information to sign privacy and accountability statements that warn of possible disciplinary action for unauthorized release of that information;
- requiring supervisory approval before SSNs are transported outside agency facilities;
- establishing and communicating written procedures regarding the labeling, storage, and disposal of SSNs and other personally identifiable data; and
- eliminating unnecessary printing and displaying of SSNs on forms, reports, and computer display screens.

The Social Security Administration Office of the Inspector General (SSA OIG) examines certain public entities that collect SSNs. Based on the SSA OIG's recommendations, the SSA educates these entities about the risks of SSN collection, use, and disclosure, and discourages the use of SSNs as a primary identifier when another identifier would suffice. The SSA OIG has released audit reports reviewing the access, use, and disclosure of SSNs by federal agencies, universities, hospitals, prisons, and state and local governments.[6]

▶ *Require Agencies To Review Their Use of SSNs*

The Task Force recommended that OMB complete its analysis of a government-wide survey it conducted regarding federal agency use of SSNs. OMB has finished its analysis and, based in part on that analysis, issued a memorandum in May 2007 to all executive departments and agencies titled "Safeguard-

ing Against and Responding to the Breach of Personally Identifiable Information" (M-07-16).[7] This memorandum requires agencies to review their use of SSNs and, among other things, identify instances in which collection or use is unnecessary. It also requires agencies to establish a plan to eliminate the unnecessary collection and use of SSNs within 18 months. In accordance with recent OMB instructions, agencies must submit their most up-to-date implementation plans for eliminating unnecessary use of SSNs and other PII as part of their annual privacy and information security reporting in October 2008.[8]

As directed by OMB, many Task Force member agencies have reduced significantly their unnecessary collection and use of SSNs. These agency-specific efforts have included removing SSNs from many internal human resource forms, reducing the use of SSNs in litigation briefs and Freedom of Information Act correspondence, partially redacting SSNs in certain types of public records, and monitoring electronic mail gateways for patterns resembling SSNs. For examples of some of these initiatives, see the Appendix.

▶ *Establish a Clearinghouse for Agency Practices That Minimize Use of SSNs*

To encourage agencies to share best practices on minimizing the use of SSNs, the Task Force recommended that the SSA develop a clearinghouse to promote successful government initiatives in this area and to facilitate information sharing. This recommendation was intended to build upon OMB's recent review of how agencies use SSNs, as well as to leverage successful efforts across the federal government.

The SSA implemented this recommendation in two steps. First, it formed the SSN Best Practices Collaborative, which included representatives from 36 federal departments and agencies that met regularly in 2007 to explore, develop, and share best practices for reducing reliance on SSNs. The Collaborative formed a subcommittee chaired by the IRS and comprised of agencies that handle high volumes of SSNs and PII, such as the Department of Defense (DOD), Department of Veterans Affairs (VA), the Department of Homeland Security (DHS), the Centers for Medicare and Medicaid Services (CMS), and SSA. Second, the SSA established a clearinghouse on a bulletin board website in July 2007; over 25 agencies have registered as users to date. The clearinghouse, which remains operational, provides a forum to share materials regarding SSN use and display by federal agencies. It showcases best practices and relevant new items, as well as contacts for specific programs and initiatives.

▶ *Work with State and Local Governments To Review Use of SSNs*

The Task Force recommended that its members work with state and local governments to highlight the vulnerabilities created by SSNs and explore ways to eliminate their unnecessary use and display. In 2007, Task Force member agencies conducted outreach to state and local governmental entities in a number of ways. For example, the Federal Trade Commission (FTC) testified before the Ohio and Maryland legislatures regarding steps that the public sector can take to prevent identity theft, including reducing the widespread availability of SSNs in public records, in particular online records.[9] The testimony also highlighted several Task Force initiatives that could be applied at the state and local levels.

In July 2007, FTC staff participated in a roundtable forum on identity theft and cybercrime hosted by the National Governors Association's National Strategic Council on Cyber and Electronic Crime. Participants discussed the need for increased collaboration both among the states and with the federal government on protecting SSNs and further research to identify the most serious threats posed by emerging technologies. In November 2007, FTC staff attended the annual meeting of the National Conference of State Legislatures and provided information about ways the states can reduce the risk of identity theft.[10] In February 2008, the FTC's Chief Privacy Officer addressed the National Association of Secretaries of State with guidance on reducing unnecessary uses of SSNs, improving data security, and developing a data breach response plan. The FTC will continue to seek opportunities to work with state and local officials and policymakers to promote these messages.

The SSA also has been active in promoting guidance about SSNs to state and local officials. For example, in 2007, an SSA official appeared before the State of Florida's Open Records Commission to provide information on SSN protection and usage. In May 2007, an SSA OIG Audit Director discussed the need to decrease the unnecessary use of SSNs in a speech before the Philadelphia Association of Government Accountants, which was attended by federal, state, and private sector auditors. SSA staff also promotes proper use of SSNs to state and local governments during information security compliance discussions and visits to SSA's data exchange partners. In addition, in September 2007, SSA OIG provided a copy of its audit report, "State and Local Governments' Collection and Use of Social Security Numbers,"to each of the 50 state governors.[11] The report recommended limiting the use of SSNs in state programs, including public K-12 schools and in UCC filings posted on the Internet, and suggested that federal laws be proposed to reduce such uses.

The IRS has been working closely with state and local agencies to safeguard taxpayers' SSNs. For example, the IRS Office of Safeguards (Safeguards) oversees the protection of federal tax information, including SSNs, provided to more than 300 local, state, and federal agencies. In December 2007, Safeguards released a revised version of Publication 1075, Tax Informa-

tion Security Guidelines for Federal, State and Local Agencies and Entities, which extended the reach of Federal Information Security Management Act (FISMA) security controls to local and state agencies that receive federal tax information.[12] Safeguards conducts approximately 100 reviews annually to ensure that these agencies comply with Publication 1075. Additionally, the IRS has implemented encrypted electronic data transmissions with state and local agencies where feasible.

RECOMMENDATION 2: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

See infra Recommendation 11, p. 23.

RECOMMENDATION 3: EDUCATE FEDERAL AGENCIES ON HOW TO PROTECT THEIR DATA AND MONITOR COMPLIANCE WITH EXISTING GUIDANCE

The Task Force also recommended that OMB continue to provide specific guidance to federal agencies on improving data security. The Task Force suggested that this guidance take the following forms.

Develop Concrete Guidance and Best Practices

The Task Force recommended that OMB and DHS develop a list of common risks to avoid in protecting sensitive personal information, as well as best practices to help avoid those risks. In 2007, OMB and DHS issued a memorandum to all federal Chief Information Officers (CIOs) listing ten common data security risks and associated best practices.[13] The memorandum identifies risks in a variety of contexts, including security and privacy training, contracts and data sharing agreements, and physical security of information, and provides links to resources for addressing those risks.

In addition, the FTC has conducted, and is continuing to conduct, extensive outreach to other federal agencies to share best practices and offer guidance on privacy, data security, and incident response. In the past year, for example, the FTC's Chief Privacy Officer delivered over a dozen presentations to more than 2,000 privacy and security professionals from across the government, offering advice on how to protect sensitive data and reduce the risk of identity theft.[14]

Comply with Data Security Guidance

The Task Force recommended that OMB continue to track and report on agency compliance with privacy and data security directives via quarterly scorecards. OMB issues these scorecards pursuant to the President's Management Agenda, which requires agencies to report quarterly to OMB on selected

performance criteria in five areas ranging from financial management to E-government initiatives.[15] Since 2002, OMB has issued scorecards that rate agencies on their status in these areas and their progress in meeting certain goals. The E-government scorecard addresses compliance with privacy and data security directives.

In each agency's E-government scorecard for the third quarter of fiscal year 2007, OMB required agency CIOs to certify compliance with OMB's May 2007 memorandum titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (M-07-16).[16] As discussed above, this memorandum required agencies to take additional steps to safeguard against and respond to the breach of PII, such as eliminating unnecessary SSN usage and developing a breach notification policy. Due to agency difficulties certifying compliance, OMB required agencies in their fourth quarter scorecards to submit status updates by December 14, 2007 and provide dates by which each agency would be in full compliance with the memorandum requirements.

In addition, OMB continues to monitor agency progress in complying with information security laws and policies through quarterly metrics that the agencies submit to OMB measuring their implementation of FISMA. The policy and guidance framework established under FISMA requires risk-based and cost-effective information security controls for systems that process or maintain federal information. Each year, OMB asks the agencies' Inspectors General (IGs) to assess the effectiveness of key agency security processes.

For the fiscal year 2007 reporting cycle, OMB asked agency IGs to assess the quality of agency processes for developing Privacy Impact Assessments (PIAs), which are required by federal law.[17] In brief, PIAs require agencies to examine the risks of collecting, maintaining, and disseminating information in identifiable form in a federal electronic information system, and require agencies to identify and evaluate protections and alternative processes to mitigate the impact on privacy. For fiscal year 2007, 19 of 23 IGs rated their agency PIA processes as "Satisfactory" or better.

OMB is requiring agencies to report additional privacy information in their fiscal year 2008 annual FISMA and privacy management report. This information must include the number of privacy reviews conducted in the last fiscal year, a description of advice provided by Senior Agency Officials for Privacy, the number of written complaints for each type of privacy issue allegation, and the number of complaints an agency referred to another agency with jurisdiction. These new requirements are described more fully in OMB's July 2008 memorandum titled "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" (M-08-21).[18] Agencies also must submit up-to-date privacy policy documents, including breach notification policies and policies outlining employee rules of behavior for handling PII.[19]

The need to protect mobile devices and media also was stressed in the FTC's outreach to privacy and security professionals in the federal government. FTC staff has urged these professionals to disseminate to agency employees an FTC-developed online tutorial that offers interactive training on this subject at *www.onguardonline.gov/laptop*.

▶ *Protect Portable Data Storage and Communication Devices*

The Task Force noted the particular vulnerabilities of laptops and other portable data storage and communication devices to theft or loss and emphasized the responsibility of each federal agency to protect such devices. OMB covered this topic in its May 2007 memorandum titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (M-07-16).[20] This memorandum reminded agencies to encrypt all data maintained on mobile computers and devices carrying agency data, unless the data is determined in writing not to be sensitive. Encryption must be certified under National Institute for Standards and Technology (NIST) Standard 140-2 to ensure that the encryption algorithm used in the product is secure. OMB also discussed agencies' obligations to protect sensitive information, including sensitive PII, on portable data storage devices in its June 2006 memorandum titled "Protection of Sensitive Agency Information" (M-06-16).[21]

In each agency's scorecard, OMB required CIOs to certify that they had reminded agency staff to protect laptops and other portable data storage and communication devices. This action was completed by CIOs for each of the scorecard agencies by the end of the first quarter of fiscal year 2008.

▶ RECOMMENDATION 4: ENSURE EFFECTIVE, RISK-BASED RESPONSES TO DATA BREACHES SUFFERED BY FEDERAL AGENCIES

The Task Force recognized that any comprehensive information security program—whether in the public or private sector—must include policies for responding to a data breach. Although every breach is different, experience has shown that having policies in place in advance is critical in ensuring a proper response. Such policies should address whether, how, and when to inform affected individuals of the loss of their data, and whether to offer services such as free credit monitoring to those individuals.

▶ *Issue Data Breach Guidance to Agencies*

The Task Force developed guidance that OMB issued to all agencies and departments on September 20, 2006 on responding to data breaches that pose a risk of identity theft.[22] The guidance provided agencies with a framework for conducting an analysis of the breach to determine whether the incident posed a significant risk of identity theft, and offered practical advice on implementing a breach response plan, including how and when to provide effective notice to affected individuals.

To further the goals of the guidance, OMB issued a memorandum to all executive departments and agencies in May 2007 titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (M-07-16).[23] Among other things, this memorandum required agencies to develop a

breach notification policy within 120 days of the memorandum's date. In addition, the memorandum provided a framework for agencies to develop such policies, based in part on the Task Force's September 2006 guidance. The memorandum also emphasized agencies' responsibilities under existing laws, such as the Privacy Act of 1974, to safeguard personally identifiable information appropriately.[24]

Publish a "Routine Use" Allowing Disclosure of Information Following a Breach

The Privacy Act prohibits federal agencies from disclosing certain information about individuals to third parties unless the individual consents or the disclosure falls within one of 12 statutory exceptions.[25] The Task Force recommended that federal agencies, in accordance with subsection (b)(3) of the Privacy Act exceptions, publish a "routine use" permitting the agencies to disclose information to appropriate third parties in the event of a breach for purposes of remediating the impact on individuals. Such a routine use would allow agencies to respond quickly and effectively to breaches in instances when the sharing of information with another agency or institution would permit prompt notification to affected individuals or would mitigate the risks associated with the breach. For example, an agency that has lost data such as bank account numbers might want to share that information with the appropriate financial institutions, which could assist in monitoring for bank fraud and in identifying the account holders for possible notification. On January 25, 2007, the Department of Justice (DOJ) published such a routine use that is also the model language for agencies to implement similar changes to existing system of records notices.[26] Many federal departments and agencies have now published notifications in the Federal Register of such a routine use.[27]

Laptop Security Tips

How to Keep It from Getting Lost or Stolen

- **Treat your laptop like cash.**
- **Get it out of the car...** don't ever leave your laptop behind.
- **Keep it locked...** use a security cable.
- **Keep it off the floor...** or at least between your feet.
- **Keep passwords somewhere else...** not near the laptop or case.
- **Don't leave it "for just a sec"...** no matter where you are.
- **Pay attention in airports...** especially at security.
- **Use bells & whistles...** if you've got an alarm, turn it on.

RECOMMENDATION 5: ESTABLISH NATIONAL STANDARDS EXTENDING DATA PROTECTION SAFEGUARDS REQUIREMENTS AND BREACH NOTIFICATION REQUIREMENTS

At present, there is no single data security or breach notification standard that applies in the United States. Rather, there is a patchwork of state laws and sector-specific federal laws and regulations that are varied and have uneven application. The Task Force recommended the development of national data security and breach notification standards that would apply to all private entities that hold sensitive consumer information. The recommended standards would direct covered entities to establish reasonable safeguards for sensitive information and to provide notification of data breaches when appropriate, while allowing for flexibility to account for, among other things, the different sizes and types of entities covered and the type of data at issue. The Task Force also recommended that the national standards be consistent with and not displace rules, regulations, guidelines, standards, or guidance applicable to financial institutions under the Gramm-Leach-Bliley Act (GLB Act).

Since the release of the Strategic Plan, Task Force members have continued to support comprehensive national data protection standards.[28] As of the date of this report, various legislative proposals for national data safeguards and breach notification standards have been introduced in Congress.

RECOMMENDATION 6: BETTER EDUCATE THE PRIVATE SECTOR ON SAFEGUARDING DATA

Because identity theft depends on access to sensitive consumer data, the Task Force recognized that those who maintain such data play a significant role in preventing identity theft. Accordingly, the Task Force recommended that, in addition to the government doing more to educate itself, it also do more to educate the private sector and consumers about the importance of data security. With respect to the private sector, the Task Force made two specific recommendations: (1) hold regional seminars for businesses on safeguarding information and (2) distribute improved guidance for private industry in developing an information security program tailored to their needs.

Hold Regional Seminars for Businesses on Safeguarding Information

Many Task Force agencies continue to provide training and outreach to the private sector on data security. The FTC developed a plan to conduct a series of data security workshops for businesses in locations around the country. The first workshop, entitled "Protecting Personal Information: Best Practices for Business," was held on April 15, 2008 in Chicago with over 250 attendees.[29] This workshop was hosted by the FTC and co-sponsored by the International Association of Privacy Professionals (IAPP) and Northwestern University School of Law. The workshop included panel discussions of key data security topics including the legal and economic risks of data breaches, how to build a culture of security within an organization, how to prepare for and respond to breaches, and how to help identity theft victims. Panelists included corporate officials, attorneys, government officials, privacy officers, and other experts.

The FTC held a second data security workshop in Los Angeles on August 13, 2008, which was co-hosted by the California Office of Privacy Protection.[30] Like the Chicago workshop discussed above, this workshop focused on how businesses can secure the personal information of consumers and employees, and it was presented in partnership with the IAPP and the Los Angeles Area Chamber of Commerce.

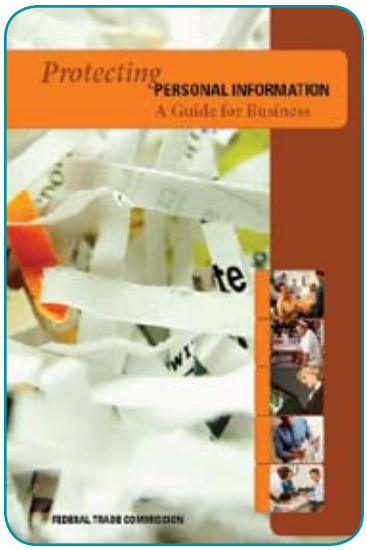
Distribute Improved Guidance for Private Industry

In recent years, Task Force members have put in place a variety of programs to educate the private sector about the importance of data security and the

risks of identity theft. This outreach effort has included business alerts, articles, testimony, tip sheets, speeches, and interviews. Over the past year, the federal depository institution regulatory agencies, through their ongoing supervisory activities, have continued to work with their regulated institutions to enhance identity theft detection, prevention, and mitigation. In addition, these agencies, through the auspices of the Federal Financial Institutions Examination Council (FFIEC), have provided information to their regulated institutions about managing risks to their operations, which include malicious activity by hackers or identity thieves. For example, in March 2008, the FFIEC issued a Business Continuity Planning Handbook for financial institutions, technology service providers, and examiners, which discusses threats to business continuity such as fraud, theft, or extortion.[31] Staff from the federal depository institution regulatory agencies also frequently speak at financial industry conferences on topics related to data security and identity theft.

Other Task Force member agencies regularly conduct outreach to the business community regarding the importance of data security and the risks of identity theft. For example, in 2007, the U.S. Postal Inspection Service gave identity theft presentations to the National Retail Federation, the National Association of Federal Credit Unions, and the International Association of Property Crimes Investigators. The U.S. Secret Service, FBI, and DOJ also speak regularly to industry groups about identity theft and cybercrime. The SSA's Office of Communications partnered with the American Association of College Registrars and Admissions Officers to encourage educational institutions to avoid using the SSN as a student identifier. In addition, an SSA OIG representative participated in a statewide outreach effort on identity theft by the Washington State Attorney General's Office, explaining the importance of shredding confidential documents.

In 2007, the FTC developed and published guidance that is the centerpiece of the FTC's data security outreach effort for businesses. Titled *Protecting Personal Information: A Guide for Business*, this plain-language brochure offers businesses practical tips on securing sensitive data, based on the principle that many breaches can be prevented by commonsense measures that are relatively simple to implement. The Guide is designed to provide businesses, both large and small, with a five-step approach to building an effective information security program. Any business or office that keeps personal information should (1) take stock of the consumer information that it collects and stores, (2) scale down the information that it keeps, (3) protect that information, (4) properly dispose of the information it no longer needs, and (5) plan ahead for potential data breaches. The Guide is available in both English and Spanish and can be downloaded easily for free in brochure format at ***www.ftc.gov/infosecurity***. The Guide is one of the most popular FTC business publications. Since its release in March 2007, the FTC has distributed over 244,000 copies of the Guide, and the online version has been accessed over 66,000 times.



In December 2007, the FTC posted on its website an interactive tutorial based on the *Protecting Personal Information* guide. The tutorial is targeted to small businesses, which can use it in developing a data security plan and to train employees. The tutorial features an FTC attorney and actors who portray business people discussing basic data security issues in plain language and across a variety of settings. The tutorial has been accessed 22,000 times since December 2007.

In December 2007, the International Association of Chiefs of Police and Bank of America posted a link to the FTC's brochure, *Protecting Personal Information—A Guide for Business*, on their partnership website, *www.idsafety.org*.

In November 2007, the FTC and the federal depository institution regulatory agencies issued final rules on identity theft "red flags" and address discrepancies to implement Sections 114 and 315 of the FACT Act. The rules require financial institutions and creditors to develop and implement an Identity Theft Prevention Program for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. The agencies also issued guidelines to assist covered entities in developing and implementing a Program, including a supplement that provides examples of red flags. Covered financial institutions and creditors must comply with the rules by November 1, 2008.

In April 2007, the FDIC issued a new policy statement reminding the institutions under its supervision of the various standards they are expected to meet to protect consumers' sensitive information and accounts and to prevent and detect identity theft. [34]

In addition, the FTC has released nine articles for businesses relating to basic data security issues for a non-legal audience.[32] The articles have been posted on a number of websites for businesses, including Dell.com's small business site, and reprinted in newsletters for local Chambers of Commerce and other business organizations.

The FTC regularly alerts businesses to specific data security topics relevant to identity theft prevention. For example, the agency mounted a nationwide campaign in December 2007 to remind businesses of their duty to truncate credit and debit card numbers on customers' purchase receipts.[33] This duty arises out of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) amendments to the Fair Credit Reporting Act (FCRA) and is intended to reduce the risk of fraud and identity theft. Under the law, businesses may not include more than the last five digits of the card number or the expiration date on electronically-printed credit and debit card receipts given to consumers. The FTC's campaign included sending the FTC's Business Alert, "Slip Showing?," to 187 national trade associations.

RECOMMENDATION 7: INITIATE INVESTIGATIONS OF DATA SECURITY VIOLATIONS

The Task Force recommended that government agencies continue to investigate and, where appropriate, take enforcement action against entities that violate data security laws and regulations. Since the release of the Strategic Plan, federal agencies have continued to bring civil and administrative actions involving data security violations. For a general description of federal efforts in the past year to investigate and bring criminal actions involving data security and identity theft, see *infra* Recommendation 25, pp. 37–41.

The federal depository institution regulatory agencies continue to investigate and to take appropriate actions against data security breaches at the institutions they supervise, including enforcement actions against financial institution insiders who breach their duty of trust to customers, engage in identity theft-related activities, or are otherwise involved in serious breaches, compromises, or misuse of customer information. These enforcement actions, among other things, have resulted in prohibitions on individuals working in the financial services industry, personal cease and desist orders restricting the use of customer information, the assessment of significant civil money penalties, and orders requiring restitution. The agencies also have taken informal and formal enforcement actions against institutions that fail to develop and properly implement a comprehensive written information security program.

The Federal Reserve Board (Board), the FDIC, the Office of Thrift Supervision (OTS), and the Office of the Comptroller of the Currency (OCC) each have established a database to track notices of security incidents submitted by supervised financial institutions pursuant to the agencies' "Guidance on Response Programs for Unauthorized Access to Customer Information and

Customer Notice (Response Program Guidance)."[35] These databases will help ensure that institutions take appropriate action to secure customer information and provide customer notice when warranted.

The FTC has made data security one of its top enforcement priorities. In the past year, it has brought six new enforcement actions against companies that allegedly failed to take reasonable measures to protect sensitive consumer data, bringing the total of FTC data security cases to 20.[36] The alleged security inadequacies in these cases ranged from disposing of sensitive documents in publicly-accessible dumpsters, to failing to implement protections against common electronic attacks, to not adequately controlling access to databases containing sensitive consumer data. In each of these cases, the company settled the charges by agreeing to implement a comprehensive data security program for which it must obtain biennial, independent assessments. The FTC currently is conducting a number of nonpublic data security investigations.

In December 2007, the FTC announced a settlement with mortgage broker American United Mortgage Co. resolving allegations that it left sensitive consumer loan documents in and around an unsecure dumpster and otherwise failed to protect customer information.[37] The case, the first to allege violations of the FTC's Disposal Rule under the FCRA, also alleged violations of the Gramm-Leach-Bliley Act (GLB Act) Safeguards and Privacy Rules. As part of this settlement, American United paid a $50,000 civil penalty for alleged Disposal Rule violations.[38]

In March 2007, the SEC launched an initiative to combat spam-driven stock market manipulations and to protect investors from potentially fraudulent email solicitations hyping small company stocks, which included several spam-related enforcement actions.[39] These actions resulted in a 50 percent reduction in spam-related complaints to the SEC's Online Complaint Center. The SEC's effort also was credited for a significant reduction in financial spam in a report by a private-sector Internet security firm.[40]

Also in 2007, the SEC and its Office of Internet Enforcement concentrated significant efforts to combat the growing threats of identity theft and account intrusions. One case resulted in the capture of $3 million in a Latvian-based bank's trading account—one of the largest asset freezes in the SEC's history.[41] Another landmark case, brought in conjunction with the Fraud Section and the Computer Crime and Intellectual Property Section of DOJ's Criminal Division and the U.S. Attorney's Office for the District of Nebraska, marked the first joint criminal and civil prosecution of a brokerage account intrusion.[42]

RECOMMENDATION 8: INITIATE A MULTI-YEAR PUBLIC AWARENESS CAMPAIGN

Recognizing that the first line of defense against identity theft often is an aware and motivated consumer, the Task Force recommended that its members initiate a broad, multi-year national public awareness campaign to educate consumers about identity theft. The Task Force carried out an extensive public awareness campaign in 2007.

The cornerstone of this effort is the FTC's "Deter, Detect, Defend: AvoID Theft" campaign, which reaches a variety of audiences through a website, articles, brochures, speeches, public service announcements, and interviews. By recommending that the public awareness program be based on the Deter,

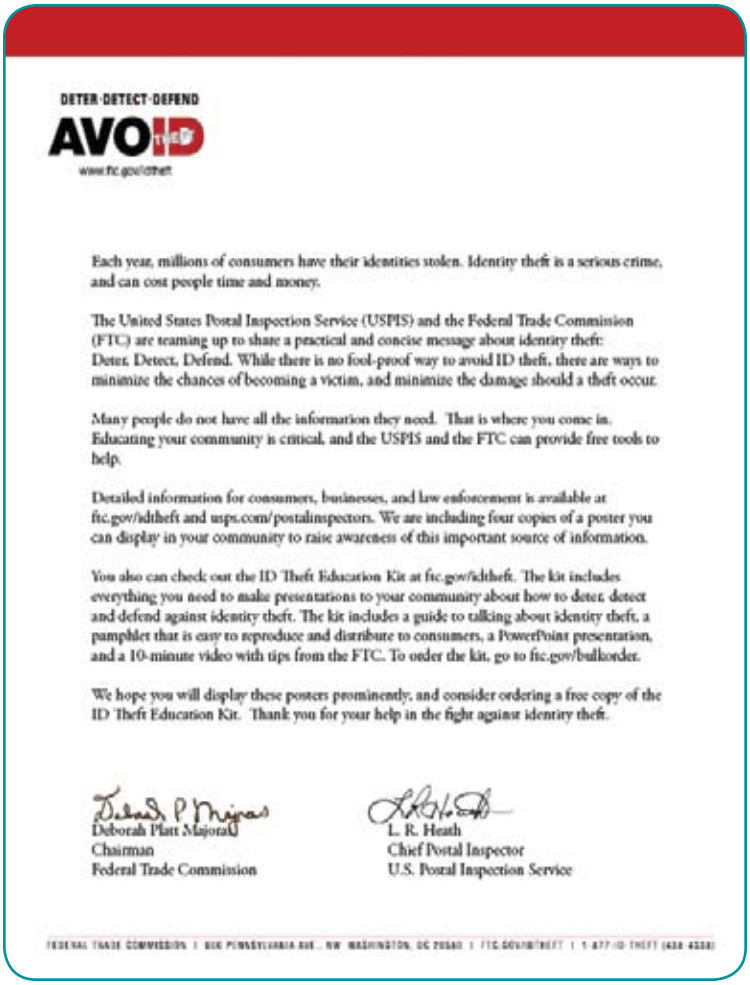
DETER·DETECT·DEFEND
AVOID THEFT
www.ftc.gov/idtheft

Detect, Defend campaign, the Task Force sought to reinforce that campaign's basic message: Consumers should take simple steps to reduce their risk of identity theft, such as securing their personal information and monitoring their credit reports and accounts.

To ensure that the campaign has the broadest possible reach, the Task Force recommended the following elements:

▶ *Develop a Broad Awareness Campaign*

The Task Force recommended that the campaign be conducted through multiple channels and that it address identity theft from a variety of perspectives, from prevention through mitigation and remediation. Over the past year, Task Force members expanded their consumer education activities in a variety of ways. Indeed, the campaign already has reached every U.S. household. In February 2008, the U.S. Postal Service, in cooperation with the FTC, delivered the Deter, Detect, Defend identity theft brochure to over 146 million residences and businesses with a cover letter from Postmaster General John E. Potter that urged consumers to protect themselves from identity theft.



DETER·DETECT·DEFEND
AVOID THEFT
www.ftc.gov/idtheft

Each year, millions of consumers have their identities stolen. Identity theft is a serious crime, and can cost people time and money.

The United States Postal Inspection Service (USPIS) and the Federal Trade Commission (FTC) are teaming up to share a practical and concise message about identity theft: Deter. Detect. Defend. While there is no fool-proof way to avoid ID theft, there are ways to minimize the chances of becoming a victim, and minimize the damage should a theft occur.

Many people do not have all the information they need. That is where you come in. Educating your community is critical, and the USPIS and the FTC can provide free tools to help.

Detailed information for consumers, businesses, and law enforcement is available at ftc.gov/idtheft and usps.com/postalinspectors. We are including four copies of a poster you can display in your community to raise awareness of this important source of information.

You also can check out the ID Theft Education Kit at ftc.gov/idtheft. The kit includes everything you need to make presentations to your community about how to deter, detect and defend against identity theft. The kit includes a guide to talking about identity theft, a pamphlet that is easy to reproduce and distribute to consumers, a PowerPoint presentation, and a 10-minute video with tips from the FTC. To order the kit, go to ftc.gov/bulkorder.

We hope you will display these posters prominently, and consider ordering a free copy of the ID Theft Education Kit. Thank you for your help in the fight against identity theft.

Deborah Platt Majoras
Chairman
Federal Trade Commission

L. R. Heath
Chief Postal Inspector
U.S. Postal Inspection Service

The Task Force continued to use the Internet as a primary means of providing identity theft information to the public. The Task Force's clearinghouse website, ***www.idtheft.gov***, contains a variety of educational resources for consumers on preventing identity theft, avoiding common scams like phishing, and protecting personal information. This site, which is discussed in more detail in Recommendation 9, also contains information on victims' rights and complaint filing procedures, as well as background on the Task Force itself. The site currently contains links to over 40 educational resources from federal government sources.

Another source of identity theft information for consumers is the FTC's website, ***www.ftc.gov/idtheft***, which features the Deter, Detect, Defend campaign. This site is updated continually and contains practical, plain-language materials—including articles, videos, forms, and sample letters—for consumers, businesses, and law enforcement. The site addresses topics ranging from how to avoid becoming an identity theft victim to steps to take if you are a victim. A recent addition to the site is an article that discusses the

many identity theft protection products on the market.[43] In fiscal year 2007, the site received over 5 million visits.

Other Task Force members, such as the Department of the Treasury, the SSA, and the U.S. Postal Inspection Service, have created web pages and publications to educate consumers about identity theft.[44] The U.S. Secret Service also recently updated its website to include detailed FAQs for consumers on identity theft.[45] The Internal Revenue Service informs taxpayers about identity theft and phishing protection via its ***www.irs.gov*** web page and asks them to report phishing incidents to its ***phishing@irs.gov*** email box. In 2007, more than 55% of IRS phishing site leads came from the general public through ***phishing@irs.gov***.

With respect to off-line efforts, the SSA has added identity theft prevention tips to its Social Security Statement, received by more than 140 million people every year, and its annual cost-of-living adjustment notices, sent to over 50 million people each December. In 2007, the SSA also updated its publication, *Identity Theft and Your Social Security Number*, which is distributed to the public through the Federal Citizen Information Center.[46] The SSA OIG also redesigned its Identity Theft pamphlet, which it provides to all victims of identity theft who contact the SSA OIG.

The federal depository institution regulatory agencies provide consumer information about identity theft on their websites, including links to information maintained by other agencies. For example, the Board and the OCC recently have established comprehensive consumer help websites, designed to provide information to consumers about financial issues, including information about identity theft.[47] The OTS added links on its website to provide consumers with information about identity theft, and it makes "camera-ready" brochures on phishing available for institutions to print and distribute to customers.[48] The FDIC continues to offer its online training tool entitled "Don't Be an Online Victim: How to Guard Against Internet Thieves and Electronic Scams."[49] To date, it has been viewed almost 75,000 times on the Internet, and the FDIC has distributed approximately 30,000 free CD-ROMs. Approximately 100 financial institutions link directly to this part of the FDIC's website.

In August 2007, the SEC's Office of Investor Education posted on the SEC's website updated information for investors titled "Phishing Fraud: How to Avoid Getting Fried by Phony Phishermen," which offers practical tips on identifying, protecting against, and responding to phishing scams.[50]

The FTC distributed 3 million print publications to consumers about identity theft in fiscal year 2007. In calendar year 2007, the U.S. Secret Service printed 45,000 copies of the FTC's "Take Charge: Fighting Back Against Identity Theft" booklet for its field offices to distribute at presentations, and it plans to print another 45,000 booklets for dissemination to the public in 2008. The SSA also has provided hard copies of the FTC identity theft materials to its regional offices for distribution across the country.

Many other agencies have distributed the FTC's identity theft publications in the past year. They include the FBI, FDIC, IRS, DOT, and the U.S. Postal Service, as well as many state attorneys general, police departments, and Congressional offices. For example, the Federal Reserve Bank in San Francisco organized an Information Security Week in October 2007 at which it distributed 2,000 Deter, Detect, Defend brochures in English and 200 in Spanish. The Missouri Department of Revenue distributed 5,000 English and 500 Spanish copies of the Deter, Detect, Defend brochure at its 183 contract license offices throughout the state.

Task Force members also continue to distribute materials designed to assist individuals in educating others about identity theft. Since April 2007, the FTC has distributed more than 31,000 AvoID Theft Consumer Education Kits to the public in English and over 2,800 kits in Spanish. These kits assist consumers in giving presentations to their own communities on avoiding identity theft. They include a victim recovery guide, a training booklet, a guide to talking about identity theft, presentation slides, an easy-to-read brochure, and a 10-minute video. The kit is available at ***www.ftc.gov/idtheft***.[51]

▶ *Enlist Outreach Partners*

The Task Force recommended that its members enlist the help of outreach partners to raise public awareness about identity theft. Over the past year, Task Force members reached out to and shared materials with numerous businesses, industry associations, non-profit groups, and law enforcement agencies, many of which spread the Deter, Detect, Defend message to their members or constituents. For example, the Washington Metropolitan Area Transportation Authority placed identity theft public service advertisements on Metro buses and rail stations in the summer of 2007. Wal-Mart printed its own Deter, Detect, Defend posters and ordered identity theft brochures for its employees.

In addition, the FTC focused on raising identity theft awareness amongst military personnel and their families, who are at a higher risk of becoming victims.[52] In 2007, the FTC worked with the U.S. Naval Media Center, which produces the Navy's internal television, radio, and print communications, to create identity theft-related television and radio news items, video clips, pod-

casts, articles, and Internet posts for sailors, civilian employees, family members, and retirees around the globe. The FTC also provided its AvoID Theft Consumer Education Kit to trade associations for military credit unions and banks for distribution to their members.

The FTC has continued its partnership with the technology sector and other federal agencies by sponsoring a multimedia website, ***www.OnGuardOnline.gov***, that educates consumers about staying safe online by, among other things, not disclosing personal information to potential fraudsters. The site contains a page devoted to consumer education about identity theft.[53] Since its launch in September 2005, OnGuardOnline has attracted more than 7 million unique visits to its website.

Law enforcement has worked together with private industry to create an educational website, ***www.LooksTooGoodToBeTrue.com***. The website was designed to educate consumers and help them avoid Internet fraud schemes, including those that can lead to identity theft. The website was developed and is maintained by a joint federal law enforcement and industry task force. Funding for the site has been provided by the U.S. Postal Inspection Service and the FBI. Key private sector partners include the National White Collar Crime Center, Monster.com, Target, and members of the Merchants Risk Council.

▶ *Increase Outreach to Traditionally Underserved Communities*

The Task Force recommended that its members increase outreach to communities that are traditionally underserved, including non-English speakers. All of the materials distributed by the FTC—consumer education kit, booklets, brochures, slides, and posters—are available in Spanish. The FTC has reached out to this community over the past year in numerous ways, including mailing 1,200 Spanish-language consumer education kits to community-based organizations that serve Hispanic consumers. The FTC also partnered with the Cuban American National Council to include identity theft information in the Council's Spanish-language monthly financial literacy seminars in Miami. In addition, the FTC provided training and distributed identity theft kits and brochures to 45 of the Housing Network Agencies for the National Council of La Raza (NCLR) and exhibited at NCLR's annual conference, distributing over 3,000 pieces of identity theft consumer education materials. The FTC also regularly communicates with about 1,500 Hispanic community organizations through its *¡Ojo!* newsletter.

Task Force members have partnered with other community-based organizations in an effort to reach traditionally underserved communities. For example, FTC staff provided assistance to LawHelp.org/NY, a non-profit organization that provides legal resources and legal aid referrals to low-income individuals in New York. The assistance included consultation on developing victim assistance materials and referrals to other available resources.

The SSA continued its targeted community outreach over the past year. Since 2006, for example, the SSA's Office of Communications has discussed identity theft and safeguarding SSNs in workshops for various audiences including Native Americans, Asian Americans, and older consumers.

Establish "Protect Your Identity Days"

The Task Force recommended that the public awareness campaign include "Protect Your Identity Days" to raise awareness about data security and identity theft. The FTC is developing kits to help businesses and organizations host their own Protect Your Identity Days, which will include sample press releases, proclamations, and public service announcements, as well as logos and other information and resources.

RECOMMENDATION 9: DEVELOP AN ONLINE CLEARINGHOUSE FOR CURRENT EDUCATIONAL RESOURCES

The Task Force recommended the creation of an online clearinghouse to house identity theft educational materials for consumers, businesses, and law enforcement at *www.idtheft.gov*. Task Force members established the clearinghouse in 2007, and it now contains links to over 40 educational resources from many federal agencies, including DOJ, the FTC, the Department of the Treasury, the SSA, and the U.S. Postal Inspection Service.[54] The clearinghouse's materials include basic identity theft information with prevention tips for consumers and businesses.

RECOMMENDATION 10: HOLD WORKSHOP ON AUTHENTICATION

Because developing more reliable methods of authenticating individuals' identities would make it harder for identity thieves to use stolen personal information to open new accounts or to access existing accounts, the Task Force recommended that member agencies convene a workshop focused on exploring new and better forms of authentication.

On April 23 and 24, 2007, the FTC hosted such a workshop, "Proof Positive: New Directions in ID Authentication."[55] Participants included a broad array of panelists from the public and private sectors and approximately 250 attendees who discussed current methods of authentication, what new technologies might become available, and how to encourage the development of more effective authentication tools. The record developed at this workshop and the related SSN workshop hosted by the FTC[56] will serve as the basis for recommendations from the FTC on SSN use in the private sector.

RECOMMENDATION 11: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

Because SSNs are both widely used by identity thieves and also serve many important functions to help reduce fraud and match consumers with their records, the Task Force recommended that it conduct a comprehensive review of the uses of SSNs in the private sector to evaluate their necessity.

The FTC, working with staff from the SSA, the federal depository institution regulatory agencies, the Securities and Exchange Commission (SEC), and other agencies, took a two-phase approach to developing this record. First, FTC staff invited comment on a series of questions regarding the role of SSNs in the commission of identity theft and their use by the private sector as identifiers and in the authentication process. The FTC received more than 300 comments and met with representatives from over 40 organizations that brought unique perspectives to the issue.[57]

On November 30, 2007, FTC staff released a comprehensive summary of the comments and information it had received from its outreach efforts.[58] The staff summary provides an overview of the current uses of SSNs, particularly the integral role they play as unique and permanent identifiers to link consumers to their records in our financial system. The summary also discusses the increased risk of identity theft associated with the widespread use and availability of SSNs, as well as current efforts to protect SSNs through state and federal statutes and regulations and private sector initiatives. In addition, the summary discusses potential alternatives to SSNs in both identification and authentication processes, as well as costs associated with reducing reliance on SSNs. Finally, the summary provides examples of federal and state laws that require various private sector entities to collect SSNs.

The second phase of the SSN review was a two-day workshop held at the FTC in December 2007, entitled "Security in Numbers: SSNs and ID Theft." [59] At the workshop, a wide array of stakeholders examined, among other topics, ways to make SSNs less valuable to identity thieves, including by improving authentication techniques and reducing unnecessary use and display of SSNs. The FTC is now preparing recommendations regarding whether additional steps should be taken to protect SSNs in the private sector. The November 2007 summary document and the record developed at the workshop will substantially inform these FTC recommendations.

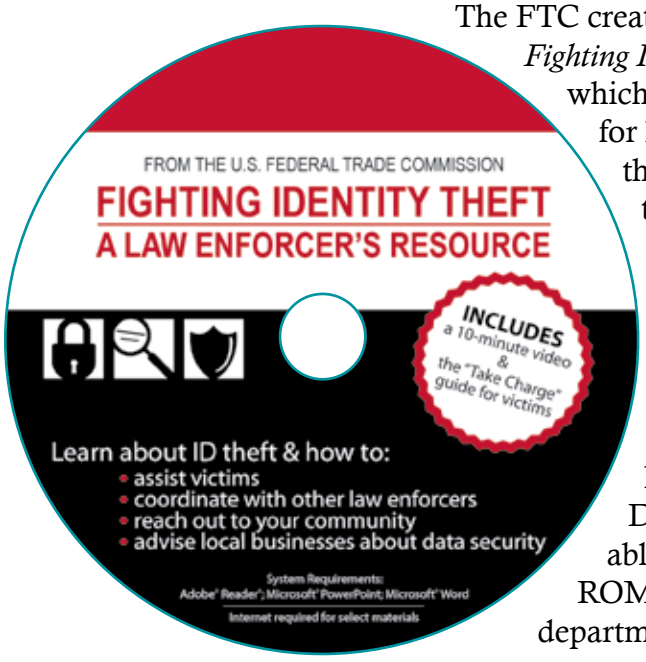
RECOMMENDATION 12: PROVIDE SPECIALIZED TRAINING ABOUT VICTIM RECOVERY TO FIRST RESPONDERS AND OTHERS PROVIDING DIRECT ASSISTANCE TO IDENTITY THEFT VICTIMS

First responders, such as law enforcement officers and others who provide direct assistance to identity theft victims, play a vital role in helping consumers recover from this crime. The Task Force emphasized the importance of training these law enforcement representatives and providing them with appropriate materials.

Train Local Law Enforcement Officers

In many identity theft cases, a victim's first step after discovering the theft is to contact local law enforcement. Therefore, it is important that local law enforcement officers are knowledgeable about the steps victims can take to begin the recovery process. In the past year, the FTC, DOJ, U.S. Secret Service, U.S. Postal Inspection Service, FBI, and American Association of Motor Vehicle Administrators have conducted seven day-long identity theft seminars for more than 900 law enforcement officers from over 250 agencies. These seminars, which covered a wide range of topics related to identity theft, contain an entire segment on helping victims begin the recovery process. The seminars stress the importance of police reports and provide access to the many victim recovery resources available to both law enforcement and victims. Additional seminars are being planned for the remainder of 2008.

Provide Educational Materials for First Responders That Can Be Readily Used as a Reference Guide for Identity Theft Victims



The FTC created a CD-ROM exclusively for law enforcement titled *Fighting Identity Theft: A Law Enforcer's Resource*. The CD-ROM, which was released in fall 2007, contains a variety of resources for law enforcement and first responders to assist victims in the recovery process, such as sample letters that can be sent to businesses requesting that they provide, without subpoena, all records related to the identity theft to both the victim and the investigating agency. The CD-ROM also offers advice on coordinating with other law enforcers, raising community awareness about identity theft, and advising local businesses about data security. Moreover, the CD-ROM contains links to relevant laws and explains how law enforcement can access the FTC's Identity Theft Data Clearinghouse, which contains over 1.6 million searchable consumer complaints. Since the release of the CD-ROM, the FTC has distributed thousands of copies to police departments across the country, as well as copies of a new poster,

What to Tell Victims of Identity Theft, that is designed to be displayed in public places.

Other FTC outreach efforts to the law enforcement community on victim assistance include an article in *Police Chief* [60] magazine about the essential role local law enforcement plays in helping identity theft victims and investigating this crime. The article also describes the free materials available to law enforcement to assist them in this mission. Following the publication of the article, hundreds of police departments requested copies of the CD-ROM and poster.

▶ Distribute an Identity Theft Victim Statement of Rights

Federal law provides certain rights to identity theft victims, such as the right to place fraud alerts on their credit reports or to block information resulting from an identity theft from their credit reports. To help educate consumers about these rights, the Task Force recommended the creation of a Victim Statement of Rights. In mid-2007, the FTC posted the Identity Theft Victim Statement of Rights to the information clearinghouse on ***www.idtheft.gov***.[61] The Statement of Rights, which describes consumers' basic rights under federal law, also has been distributed at training seminars and conferences for law enforcement officers hosted by the International Association of Chiefs of Police and the International Association of Financial Crime Investigators.

▶ Develop Nationwide Training for Victim Assistance Counselors

A variety of state and federal programs, as well as non-profit organizations, provide direct assistance to identity theft victims. The Task Force recommended that member agencies develop nationwide victim assistance training for counselors at these programs. Accordingly, DOJ's Office for Victims of Crime (OVC) conducted a national training session, developed in cooperation with the FTC, for victim-witness coordinators in 2007. Attendees included law enforcement, mental health providers, victim service providers, clergy, and allied professionals.

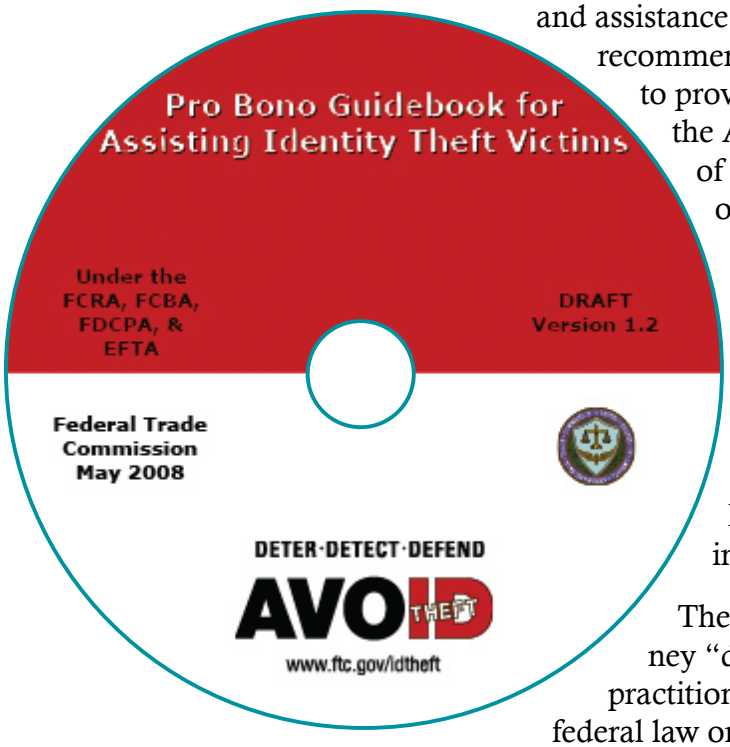
In addition, OVC offers an identity theft workshop as ongoing training on the OVC Training and Technical Assistance Center Training Workshop Calendar.[62] OVC's training calendar features action-oriented training sessions that are relevant to crime victim services. OVC also offers scholarships for victim services providers to attend relevant identity theft training nationwide.

To increase identity theft victim assistance services, OVC has encouraged Victims of Crime Act (VOCA) victim assistance administrators to expand their program outreach to identity theft victims. OVC also has highlighted identity theft and fraud issues at the VOCA Administrators' Annual Conferences by supporting victim impact workshops to help recognize the needs of identity theft victims and expand program services using VOCA victim assistance dollars.

OVC also has funded the development of a resource guide for victim service organizations on serving identity theft victims, entitled *Assisting Victims of Identity Theft: A Resource Guide for Victim Services*. OVC plans to make the publication widely available to victim service providers in 2008. OVC also recently distributed 4,600 copies of the FTC's AvoID Theft Consumer Education Kit, a training-of-trainers awareness kit, to the victim services field, VOCA administrators, and national victim-related organizations.

RECOMMENDATION 13: DEVELOP AVENUES FOR INDIVIDUALIZED ASSISTANCE TO IDENTITY THEFT VICTIMS

Engage the American Bar Association To Develop a Program Focusing on Assisting Identity Theft Victims with Recovery



Although government agencies at all levels are expanding services and assistance to identity theft victims, the Task Force also recommended that member agencies engage the organized bar to provide individualized assistance to victims. To that end, the Administrative Law and Regulatory Practice Section of the American Bar Association (ABA), in response to outreach by DOJ and the FTC, proposed a resolution that urges national, federal, state, territorial, tribal, and local bar associations, in cooperation with state and local pro bono, lawyer referral, and legal aid programs, to establish programs for representation of identity theft victims. This resolution, which was cosponsored by several ABA sections and standing committees, was approved by the ABA House of Delegates and became formal ABA policy in February 2008.

The FTC and DOJ have developed a preliminary attorney "deskbook" on identity theft, which provides pro bono practitioners with guidance on key legal issues arising under federal law on which identity theft victims may need assistance. The deskbook will provide tools and resources for pro bono attorneys to assist victims who are having difficulty clearing their credit or criminal histories. FTC and DOJ staff presented this material at a meeting of the ABA's Equal Justice Conference in May 2008. Current plans call for these materials to be provided to state and local bar associations, which could then add their own materials on state law issues to tailor the deskbook to the needs of attorneys within their respective jurisdictions. The deskbook also will be made available on ***www.idtheft.gov***.

Although this recommendation was focused on the ABA as a source for victim assistance, Task Force member agencies identified other ways to expand assistance to identity theft victims. DOJ's Bureau of Justice Assistance has provided substantial grants to organizations at the national, regional, state, and city level for programs that provide direct assistance to identity theft victims. The grant recipients are the Identity Theft Resource Center, the Victims' Initiative for Counseling, Advocacy, and Restoration of the Southwest, the Maryland Crime Victims' Resource Center, Inc., and Atlanta Victim Assistance. Each of these grantees will be developing resources, projects, and protocols that can serve as models for other victim assistance programs.

RECOMMENDATION 14: AMEND CRIMINAL RESTITUTION STATUTES TO ENSURE THAT VICTIMS RECOVER FOR THE VALUE OF TIME SPENT IN ATTEMPTING TO REMEDIATE THE HARMS THEY SUFFERED

Last year, the Senate passed S. 2168, the Identity Theft Enforcement and Restitution Act of 2007, and referred it to the House of Representatives. This bill incorporated many of the Task Force's legislative recommendations, including authority to seek restitution for identity theft victims for the value of their time spent addressing the harm they suffered, expansion of the identity theft offenses to cover prosecution for corporate identity theft, and various cybercrime-related provisions to cover malicious spyware, keyloggers, and cyberextortion that do not explicitly "damage" computers.[63] In July 2008, the Senate passed H.R. 5938, which was amended to include the cybercrime-related provisions of S. 2168, and referred it back to the House for approval.[64] DOJ provided guidance to Congressional staff on the bills' provisions, and Acting Principal Deputy Assistant Attorney General and Chief of Staff for the Criminal Division, Andrew Lourie testified on S. 2168 before a House Judiciary Subcommittee.

RECOMMENDATION 15: EXPLORE THE DEVELOPMENT OF A NATIONAL PROGRAM ALLOWING IDENTITY THEFT VICTIMS TO OBTAIN AN IDENTIFICATION DOCUMENT FOR AUTHENTICATION PURPOSES

The Task Force recommended that its member agencies study the feasibility of a national program to provide victims with an identification document, or "passport," to prove they are who they say they are. Such documentation is particularly important where a suspect has used the victim's name in the commission of a crime. Various states have developed passport programs for

identity theft victims. In addition, OVC has funded a pilot program in Ohio. Under Ohio's Identity Theft Verification Passport Program, once a police report is filed, law enforcement personnel enter the victim's information into a statewide database, where it is then forwarded to other agencies that can reduce the risk of additional fraud. Ohio's Passport Program offers victims a "passport," which they can show to creditors and law enforcement when disputing fraudulent criminal charges or claims. DOJ's OVC is evaluating the efficacy of this program, as well as the viability of the FBI's National Crime Information Center (NCIC) identity theft file as an alternative to the passport programs.

RECOMMENDATION 16: ASSESS EFFICACY OF TOOLS AVAILABLE TO VICTIMS

Identity theft victims have many rights under federal law to assist them in recovering from the crime.[65] In order to determine whether these rights are effective, the Task Force recommended that its member agencies study identity theft victims' experiences in exercising these rights. In addition, some states have adopted victim assistance measures that have no federal counterpart. The Task Force recommended that the efficacy of those measures be evaluated in order to determine whether they should be adopted at the federal level.

Conduct Assessment of FACT Act Remedies Under FCRA

The 2003 FACT Act amendments to the Fair Credit Reporting Act (FCRA) granted several new rights to identity theft victims, including the right to place fraud alerts on their credit reports, the ability to block fraudulent trade lines from credit reports, the right to have creditors cease providing information from fraudulent transactions to consumer reporting agencies, and the right to obtain business records relating to fraudulent accounts. The Task Force recommended that the agencies that enforce the FCRA conduct surveys to measure the effectiveness of these rights.

The FTC is preparing a survey of identity theft victims that will examine the experiences of victims who have attempted to exercise these rights. The survey, which will be conducted through a written questionnaire sent to identity theft victims who contacted the FTC through its complaint handling system, will ask victims about which rights they attempted to exercise, the results of those attempts, and victims' satisfaction with the identity theft recovery process. The results of this survey will be released in the fourth quarter of 2008.

Conduct Assessment of State Credit Freeze Laws

The Task Force also recommended that the FTC, with support from other Task Force members, assess the impact and effectiveness of state credit freeze laws and report on the results in 2008. This report is intended to help policy-makers determine whether a federal credit freeze law would be appropriate.

Although state credit freeze laws vary in many respects, they share a common goal: to prevent identity thieves from opening new accounts in consumers' names by restricting access to credit reports. Once a consumer initiates a credit freeze with a consumer reporting agency (CRA), the freeze prevents that CRA from releasing a credit report about that consumer unless the consumer temporarily lifts or permanently removes the freeze. Because businesses typically will not extend new credit without first viewing the consumer's credit report, credit freezes make it more difficult for identity thieves to open new accounts in consumers' names.

In January 2008, the FTC staff sought public comment on the credit freeze laws enacted by 39 states and the District of Columbia, as well as the commercially-developed credit freeze options (CDFOs) offered by the three nationwide CRAs.[66] In its request for public comment, the FTC sought responses to specific questions in addition to general information regarding the efficacy of credit freezes. The specific questions were designed to collect data on the experiences of consumers, users of credit reports, and CRAs with credit freezes. The questions also were designed to elicit information comparing credit freezes with other identity fraud prevention tools, such as fraud alerts. The FTC received over 50 comments from consumers, consumer advocates, and industry representatives. The staff report, which will be issued in 2008, will examine the features, functionality, and costs associated with using the freeze mechanism in systems developed under state law mandates as well as in CDFO jurisdictions.

RECOMMENDATION 17: ESTABLISH A NATIONAL IDENTITY THEFT LAW ENFORCEMENT CENTER

The Task Force recommended that law enforcement agencies consider the establishment of a National Identity Theft Law Enforcement Center. Such a Center would focus on the analysis of identity theft complaint data and related information and bolster the sharing of information between law enforcement officers around the country. DOJ is reviewing the feasibility and efficacy of establishing such a Center.

In the meantime, significant progress has been made in achieving greater cooperation between law enforcement agencies. For example, monthly meetings of the Task Force's Criminal Law Enforcement Subgroup bring together a

wide range of prosecutors, investigators, and analysts from agencies including DOJ's Criminal Division, U.S. Attorneys' Offices, the FBI, the Department of the Treasury, the FTC, the Diplomatic Security Service, the U.S. Secret Service, SSA OIG, and the U.S. Postal Inspection Service. The Subgroup discusses emerging trends in identity theft, shares best practices, and receives reports from government and private sector representatives involved in combating identity theft.

In addition, several databases and organizations bring together law enforcement partners in their fight against identity theft:

- The FTC's Identity Theft Data Clearinghouse is a national database available to law enforcement that contains more than 1.6 million victim complaints about identity theft. Over 1,650 federal, state, and local law enforcement and regulatory authorities have access to the Clearinghouse for purposes of conducting investigations, obtaining information about identity theft victims, and identifying other agencies involved in an investigation. The FTC also occasionally shares complaint information from the Clearinghouse with private entities in order to resolve identity theft-related issues.
- The National Identity Crimes Law Enforcement (NICLE) Network, formerly known as the Regional Identity Theft Network (RITNET), became operational in July 2008. The project originated with the United States Attorney's Office for the Eastern District of Pennsylvania in coordination with the U.S. Postal Inspection Service and the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN). The NICLE Network allows authorized law enforcement at the federal, state, and local levels to enter and retrieve identity crimes data through the Regional Information Sharing Systems Network, a centralized data sharing system. NICLE is designed to include data from the FTC, law enforcement agencies, and the banking and retail industries.[67]
- The Internet Crime Complaint Center (IC3) is another law enforcement resource. IC3 is an alliance between the FBI, the National White Collar Crime Center, and DOJ's Bureau of Justice Assistance. IC3's mission is to collect and disseminate intelligence regarding crime committed over the Internet.
- The FBI's Cyber Initiative Resource Fusion Unit (CIRFU), in conjunction with the National Cyber-Forensics and Training Alliance (NCFTA) and the U.S. Postal Inspection Service, works with the private sector to operate Identity Shield. Identity Shield is a project in which CIRFU collects PII that has been posted on the Internet by identity thieves and reports it to the major

consumer reporting agencies and affected financial institutions. CIRFU and the IC3 also work together to report the thefts to relevant law enforcement agencies.

- The National Cyber Investigative Joint Task Force (NCIJTF) helps coordinate, integrate, and share cyber threat information with the intelligence community and law enforcement.
- The FBI's InfraGard program, with more than 20,000 members, is a government and private sector alliance designed to strengthen the defense of key national infrastructures and resources through information sharing. Each of the FBI's 56 field offices has at least one InfraGard chapter within its territory. Each InfraGard chapter is comprised of critical infrastructure and resource stakeholders from the private and public sectors. The InfraGard program has enhanced the FBI's ability to gather information related to identity and PII theft and compromise, as well as other cyber threats.
- The Secret Service has established 29 Financial Crimes Task Forces and 24 Electronic Crimes Task Forces strategically throughout the United States to aid in combating identity theft. These task forces are comprised of approximately 2000 state, local, private sector, and academia partners. These task forces are an integral part of Secret Service efforts to combat identity theft.

In addition, regional and local task forces have been organized around the country to maximize talent, resources, and experience in targeting identity theft. Often, these task forces are composed of federal and local investigators and prosecutors. These collaborative efforts have made significant strides in targeting and prosecuting identity thieves through the efficient sharing of investigative leads. For more information about these task forces, *see infra* Recommendation 25, pp. 37–41.

RECOMMENDATION 18: DEVELOP AND PROMOTE THE ACCEPTANCE OF UNIVERSAL IDENTITY THEFT REPORT FORM

The Task Force recommended that its member agencies develop and promote a standard document that an identity theft victim could complete, print, and take to a local police department to be incorporated into the department's report system. This would facilitate the creation and availability of police reports, which victims need to exercise many of their FACT Act rights, such as placing a 7-year fraud alert on their credit file or blocking fraudulent information from their credit reports. In addition, other information from this universal identity theft report form could be entered into a central database used by law enforcement agencies to analyze patterns and trends and initiate identity theft investigations.

The FTC, together with criminal law enforcers and representatives of financial institutions, the consumer data industry, and consumer advocacy groups, developed a universal form that met the goals of this recommendation. In October 2006, the resulting "Identity Theft Complaint" form was made available on the FTC's website, ***www.ftc.gov/idtheft***. The form also can be accessed on the Task Force's online clearinghouse, ***www.idtheft.gov***. Since its release, Task Force members have promoted the form's use to victims, law enforcement, CRAs, and creditors. For example, FTC staff promoted the form at the International Association of Chiefs of Police (IACP) national conference and the International Association of Financial Crime Investigators (IAFCI) conference in 2007. The FTC also promoted the form to law enforcement in its article about identity theft in the December 2007 *Police Chief* magazine.[68]

RECOMMENDATION 19: ENHANCE INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND THE PRIVATE SECTOR

Because the private sector is an important source of information and assistance with respect to identity theft, the Task Force recommended several steps be taken to promote information sharing between law enforcement and the private sector.

Enhance Ability of Law Enforcement To Receive Information from Financial Institutions

Section 609(e) of the FCRA enables identity theft victims to obtain copies of records related to the theft from the businesses that dealt with the thief and to designate law enforcement agencies to receive this information on their behalf. Because law enforcement agencies sometimes have had difficulty in obtaining such information, the Task Force recommended that federal law enforcement agencies initiate discussions with the financial sector to ensure greater compliance with this law. Accordingly, several member agencies, including the FBI, the U.S. Secret Service, the U.S. Postal Inspection Service, DOJ, and the FTC, have met jointly with a number of financial services industry representatives to discuss improving communications on identity theft issues generally, and compliance with Section 609(e) of the FCRA in particular. In addition, the FTC has included a model letter and educational materials related to Section 609(e) on its website and a CD-ROM sent to law enforcement.[69] The FTC has established an email address where law enforcement personnel can report difficulties they are having in acquiring Section 609(e) information and receive assistance in resolving those difficulties.

Initiate Discussions with the Financial Services Industry on Countermeasures to Identity Thieves

The Task Force also recommended that the U.S. Postal Inspection Service continue discussions with the financial services industry to develop more ef-

fective fraud prevention measures to deter identity thieves who obtain consumer information through mail theft. In 2007, the U.S. Postal Inspection Service continued this type of collaboration with the private sector by sponsoring the Financial Industry Mail Security Initiative (FIMSI). The purpose of this initiative is to reduce fraud and theft via the mail, and its members include the U.S. Postal Inspection Service; other federal, state, and local law enforcement agencies; major commercial mailers; and representatives from the financial and retail sectors such as banks and credit card companies. In 2007, FIMSI members met regularly to exchange information about trends and developments in fraud and identity theft. In addition, FIMSI members identified and exchanged information on best practices and loss prevention strategies, as well as improved procedures to facilitate criminal investigations and prosecutions where warranted.

In 2007, the U.S. Postal Inspection Service continued to work with the private sector on countermeasures to identity theft by participating in the Intelligence Sharing Initiative (ISI). Like FIMSI, the ISI facilitates information sharing between the private sector and law enforcement. The ISI has over 200 members representing 70 major financial institutions, retail organizations, and law enforcement agencies.

In addition, the IRS has been working with the Information Reporting Program Advisory Committee (IRPAC), which is comprised of private sector entities that have reporting requirements to IRS through income and dividend notices, to assess the legal requirements and alternatives to displaying the SSN on information returns such as Form 1099.

Initiate Discussions with Credit Reporting Agencies on Preventing Identity Theft

The Task Force also recommended that DOJ and the FTC initiate discussions with the CRAs on possible measures that would make it more difficult for identity thieves to obtain credit based on access to a victim's credit report. These discussions have begun and will continue throughout 2008.

RECOMMENDATION 20: ENCOURAGE OTHER COUNTRIES TO ENACT SUITABLE DOMESTIC LEGISLATION CRIMINALIZING IDENTITY THEFT

Because identity theft has emerged as a global and transnational crime, the criminalization of identity theft by the United States' international law enforcement partners is the linchpin of an effective deterrence scheme. Further, reducing the disparity in regulatory schemes between countries promotes international cooperation. The Task Force recommended that DOJ, after consulting with the Department of State, formally encourage other countries to enact suitable domestic legislation criminalizing identity theft.

In the past year, the U.S. government has continued to reach out to its international law enforcement partners to heighten awareness of identity theft. Much of DOJ's interaction has been in formal meetings or conferences with regional law enforcement groups. Such interaction also has arisen in bilateral meetings, either during formal visits or when foreign officials visit on a more informal basis. In these latter cases, DOJ has hosted international officials and discussed identity theft and related cybercrime laws. In each of these areas over the last year, DOJ has increased its emphasis on identity theft issues.

For example, at a European Union conference in Portugal in late 2007, DOJ presented the United States' experiences with and responses to identity theft issues. The conference was perhaps the most important identity theft conference in Europe to date, bringing together experts from Europe and other parts of the world. Similarly, DOJ is a major participant in ongoing work by the United Nations Office on Drugs and Crime to foster a multilateral response to identity theft. In addition, DOJ is supporting a proposed project by the G8 Criminal Legal Affairs Subgroup pertaining to the criminalization of identity theft in various countries.[70]

RECOMMENDATION 21: FACILITATE INVESTIGATION AND PROSECUTION OF INTERNATIONAL IDENTITY THEFT BY ENCOURAGING OTHER NATIONS TO ACCEDE TO THE CONVENTION ON CYBERCRIME, OR TO ENSURE THAT THEIR LAWS AND PROCEDURES ARE AT LEAST AS COMPREHENSIVE

To facilitate investigation and prosecution of international identity theft, the Task Force recommended that the U.S. government continue its efforts to promote accession to the Council of Europe's Convention on Cybercrime (Convention). The Convention is the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks. Because the Convention includes offenses that relate to the stealing and exploitation of personal information, it ensures that all countries that are parties to it have the ability to assist effectively in transnational identity theft cases.

DOJ has taken the lead on carrying out this recommendation, in appropriate coordination with the State Department and other agencies. In the past year, DOJ's efforts to support and encourage accession to the Convention have continued and intensified on a number of fronts. Every international training program on cybercrime-related issues conducted by DOJ includes at least some discussion of the Convention; many presentations focus on it exclusively. DOJ's commitment to the Convention is evidenced by the fact that

a DOJ official serves as the chair of the Council of Europe's committee on implementation of the Convention. The United States encourages additional countries to join the Convention, and the United States recently consented to the accession of two non-European countries.

In addition, DOJ works with regional organizations, such as the Asia-Pacific Economic Cooperation forum and the Organization of American States, in support of resolutions encouraging countries to adopt the Convention or otherwise amend their laws.

RECOMMENDATION 22: IDENTIFY COUNTRIES THAT HAVE BECOME SAFE HAVENS FOR PERPETRATORS OF IDENTITY THEFT AND TARGET THEM FOR DIPLOMATIC AND ENFORCEMENT INITIATIVES FORMULATED TO CHANGE THEIR PRACTICES

The Task Force recommended that the U.S. government identify countries that have become safe havens for perpetrators of identity theft and encourage those countries to change their practices. In its enforcement and training efforts, DOJ pays special attention to countries that are significant centers of cybercrime, focusing its resources in those countries. It also has assisted the Department of State in preparing State officials to press host governments for progress in cybercrime legislation and enforcement.

RECOMMENDATION 23: ENHANCE THE U.S. GOVERNMENT'S ABILITY TO RESPOND TO APPROPRIATE FOREIGN REQUESTS FOR EVIDENCE IN CRIMINAL CASES INVOLVING IDENTITY THEFT

The Task Force recommended that the U.S. government enhance its ability to respond to appropriate foreign requests for evidence in criminal cases involving identity theft. In the past year, DOJ has worked to enhance the U.S.'s ability to respond to such requests, providing both formal and informal assistance. For example, DOJ is examining the development of innovative procedures that would allow information on U.S. victims to be gathered in a way that it could be introduced into evidence in foreign jurisdictions. In those cases where the United States is unable to obtain extradition of foreign identity theft perpetrators, DOJ intends to develop methods that would ensure that U.S. victim information is introduced into foreign prosecution proceedings. This will facilitate foreign prosecutions, increase foreign criminal sentences, and provide for the possibility of obtaining restitution for U.S. victims.

Structurally, DOJ, in coordination with the Department of State, continued its efforts to expand the "24/7 network." This network of agencies from approximately 50 participating countries provides assistance at all hours to consider other countries' requests for preservation or disclosure of electronic evidence in emergency cases. DOJ was a key participant in the founding of this network and serves as its representative for the United States. Also, DOJ assisted in integrating this G8-initiated network with a similar network started by the Council of Europe.

RECOMMENDATION 24: ASSIST, TRAIN, AND SUPPORT FOREIGN LAW ENFORCEMENT

Because of the large and growing role of international issues in all cybercrime investigations, the Task Force recommended that federal law enforcement agencies assist, train, and support foreign law enforcement in this area. DOJ has taken the lead here by partnering with the Department of State to provide extensive training for other countries to ensure that their procedural and substantive laws are adequate to address cybercrime and to assist other countries in obtaining evidence from them. DOJ trains foreign prosecutors, legislators, judges, and law enforcement agents, often under the auspices of a multilateral organization such as the Organization of American States or the Asia Pacific Economic Cooperation Forum. For example, in December 2007, DOJ sponsored credit card fraud training in Moscow for 50 police officers and investigators from the Russian Ministry of Interior. Presentations were made by DOJ prosecutors, FBI agents, and representatives of Russian banks and major credit card companies in Russia. In 2008, DOJ will conduct an ambitious cybercrime training program with emphasis on Asia, Latin America, the Caribbean, and sub-Saharan Africa.

The U.S. Secret Service also has been active in training foreign law enforcement about identity theft. In 2007, the U.S. Secret Service provided classroom instruction on identity theft at International Law Enforcement Academies (ILEAs) to over 500 foreign police officials in El Salvador, Botswana, Thailand, and Hungary. These courses focused on phishing, skimming, and retrieving identification information through computer hacking. The same number of foreign police officials will attend ILEA instruction in 2008.

The U.S. Postal Inspection Service provided training to international law enforcement by participating in the 2007 training conference of the International Association of Financial Crimes Investigators in Toronto, Canada. Over 800 law enforcement officers from around the world attended the conference, at which the Chief Postal Inspector made a presentation on identity theft and mail theft.

In addition to training, DOJ made an open offer to assist other countries with review and comment on their proposed laws on cybercrime and identity theft. DOJ has provided this service to approximately 20 countries to date.

DOJ also has led hands-on exercises that bring together law enforcement agents from different countries. For example, at a November 2007 meeting of the G8 High Tech Crime Subgroup, DOJ led a "table top" exercise concerning computer "botnets"—virtual armies of thousands of computers that have been compromised illegally and hijacked to commit identity theft and other crimes. More than 70 representatives from law enforcement, network security agencies, banks, Internet service providers, and other private sector entities from each of the G8 countries participated in the exercise, which focused on identity theft and highlighted international law enforcement and private sector cooperation.

Thirty-three members of the ring were charged in Los Angeles with 65 criminal counts, including conspiracy to violate the Racketeer Influenced and Corrupt Organizations (RICO) statute, aggravated identity theft, access device fraud, bank fraud, and computer fraud. At the same time, seven other Romanian citizens were charged with related aggravated identity theft and fraud charges in New Haven, Connecticut. This important milestone, like other recent joint operations with Romania, was achieved due to close cooperation within all levels of the U.S. law enforcement community and with our foreign partners.

This case was the result of an extraordinary joint investigation involving the United States Attorneys' Offices for the Central District of California and the District of Connecticut, the FBI, the Romanian General Inspectorate of Police, U.S. Immigrations and Customs Enforcement, the U.S. Postal Inspection Service, the Internal Revenue Service, the Connecticut Computer Crimes Task Force, and a large number of local law enforcement agencies. Additional assistance was provided by the U.S. Secret Service.

On May 19, 2008, United States and Romanian law enforcement officials announced the disruption of a major identity theft ring operating in those two countries plus several others. The group is charged with a sophisticated phishing scheme targeting the personal and financial information of large numbers of victims. The indictment charges that the group sent over a million fraudulent email messages, which ultimately resulted in victims being tricked into providing financial and identification data that was used to steal funds.

RECOMMENDATION 25: INCREASE PROSECUTIONS OF IDENTITY THEFT

Increasing the criminal deterrence of identity theft was a key Task Force recommendation. In the past year, Task Force member agencies have been active in prosecuting identity theft. DOJ has conducted numerous successful criminal prosecutions of individuals who stole consumer information. In fiscal year 2006, 1,946 defendants were charged with violating one of the two main federal identity theft statutes, and 1,534 defendants were convicted. In fiscal year 2007, 2,470 defendants were charged, and 1,943 were convicted. This was a 26.9% increase in numbers of defendants charged, and a 26.7% increase in the number of defendants convicted of identity theft.

In one such case, the defendant used file sharing programs, including the "LimeWire" program, to search for federal income tax returns, student financial aid applications, and credit reports that had been stored electronically by victims on their own private computers. He then used the identity, banking,

In United States v. Mario Simbaqueba Bonilla (S.D. Fla. Jan. 2008), the defendant pleaded guilty to illegally installing keystroke logging software on computers in hotel business centers and internet lounges around the world. The software would collect the personal information of those who used the computers, including passwords and other information the victims used to access their bank, payroll, brokerage, and other accounts online. The defendant admitted to using this data to steal or divert money from the victims' accounts into other accounts he had created in the names of other people he had victimized in the same way. In April 2008, the defendant was sentenced to nine years' imprisonment and ordered to pay restitution of $347,000 for these crimes.

financial, and credit information he had obtained to open credit accounts online in the victims' names. He was arrested in October 2007, pursuant to an indictment by a federal grand jury in the Western District of Washington for mail fraud, computer fraud, and aggravated identity theft. He was sentenced to four years' imprisonment. The defendant's scheme was linked to at least 80 victims and more than $70,000 in fraud. Other cases have involved defendants who hacked into secure computer systems to acquire consumer information or installed keystroke loggers or similar malicious software on public computers to collect consumer information.

In addition, DOJ is continuing to investigate and prosecute individuals who engage in "carding," the practice of trafficking in consumer information such as credit card account numbers and SSNs. Frequently, carders obtain their data through phishing, computer and network hacking, cashing out stolen account numbers, and reshipping schemes.[71] Individuals engaged in carding-related activity often belong to organizations that operate and maintain online "carding forums," which are dedicated to the sale of stolen personal and financial information and fraudulent identification documents.

One such criminal carding forum was managed by the "Shadowcrew" organization, against which DOJ has brought over 30 cases, which were investigated by the Secret Service's Newark Field Office. DOJ also has prosecuted the co-founder and administrator of the carding forum, "Cardersmarket," which was investigated by the Secret Service's Pittsburgh Field Office. In September 2007, the ringleader of Cardersmarket was indicted by a federal grand jury in Pittsburgh on charges of wire fraud and identity theft related to an online scheme to steal credit card and other identity information. The indictment alleges that the suspect hacked into computer systems of financial institutions and credit card processing centers in order to obtain credit card account information and other personal identification information. The buyers would either use the information themselves to make fraudulent purchases or resell it to others, causing losses to credit card issuers. According to the indictment, the suspect sold tens of thousands of stolen credit card numbers.

More recently, on August 5, 2008, the Attorney General, in conjunction with the U.S. Attorney for the District of Massachusetts, the U.S. Attorney for the Southern District of California, the U.S. Attorney for the Eastern District of New York, and the Director of the U.S. Secret Service, announced the indictment of 11 members of an international retail hacking ring charged with stealing and distributing over 40 million credit and debit card numbers from major U.S. retailers. This is believed to constitute the largest hacking and identity theft case ever prosecuted by the United States, and involves defendants from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus.

The three-year Secret Service investigation (involving the Secret Service's San Diego, Miami, and Boston Field Offices, in close coordination with the Head-

quarters Divisions) resulted in indictments in three U.S. Attorney's Offices. The conspirators were charged, among other things, with computer fraud, wire fraud, access device fraud, aggravated identity theft, and conspiracy. The indictments allege that during the course of the sophisticated conspiracy, the conspirators obtained the credit and debit card numbers by "wardriving"and hacking into the computer networks of major retailers. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. The conspirators then sold these credit and debit card numbers via the Internet to other criminals around the world who used them for identity theft, often laundering the proceeds through anonymous Internet-based currencies and foreign bank accounts.

The U.S. Secret Service has been active in investigating network intrusions and data breaches that result, among other things, in the compromise of personal information. To further its efforts in this area, the Secret Service has expanded its Criminal Intelligence Section into an investigative unit capable of combating international cybercrimes. Now called the Cyber Investigative Section, it is designed to target highly motivated and sophisticated hackers and online criminal networks that operate internationally. This will enable the Secret Service to more effectively investigate large-scale data breaches and network attacks as well as identify the tools used to commit these types of crimes. The FBI also has participated in many criminal data security investigations over the past year.

In addition to its general recommendation to increase prosecutions of identity theft, the Task Force recommended that its member agencies take specific steps to facilitate such prosecutions. These steps are discussed below.

▶ *Designate an Identity Theft Coordinator for Each U.S. Attorney's Office*

The Task Force recommended that each U.S. Attorney's Office designate an identity theft coordinator. All 93 U.S. Attorneys' Offices now have done so. Typically, this coordinator is an Assistant U.S. Attorney (AUSA) with extensive experience in prosecuting identity theft cases. These coordinators serve as liaisons between the district office and the various communities served. Federal, state, and local law enforcement agencies rely on these AUSAs for information, advice, and emergency prosecutorial decisions. This effort builds on existing programs in various U.S. Attorneys' Offices to coordinate identity theft resources.[72]

The identity theft coordinators also facilitate efficient communication between the district offices and DOJ headquarters on identity theft related matters, including law, policy, and budget issues. Ensuring that each office has a designated official to manage identity theft issues also results in better coordination with state and local officials, and among federal identity theft prosecutors nationwide.

On February 25, 2008, in Washington State, David Haltinner was sentenced to serve 50 months in prison for aggravated identity theft and access device fraud. He had used an assumed identity to sell approximately 637,000 stolen credit card numbers online. He used his position as an information security analyst to steal this information from his employer. Haltinner also was ordered to pay restitution in excess of $750,000 to cover the expenses of notifying and providing credit card monitoring services to the affected individuals.

On May 12, 2008, the U.S. Attorney for the Eastern District of Pennsylvania filed charges against Edward K. Anderton and Jocelyn Kirsch for their participation in an elaborate identity theft scheme. Anderton and Kirsch committed a variety of schemes, including burglarizing homes and impersonating a police officer, to steal personal information that they then used to buy merchandise and services. They used the identities of more than 16 victims to obtain at least $119,381 in cash and merchandise and attempted to steal another $112,621 in additional cash and merchandise. They both recently pled guilty to charges including conspiracy, aggravated identity theft, access device fraud, bank fraud, and money laundering.

In January 2008, a former Girl Scout troop leader was sentenced to 10 years in federal prison for filing false IRS claims and identity theft totaling more than $187,000. Holly M. Barnes pleaded guilty to 19 counts of filing false and fictitious tax refund claims to the IRS, 15 counts of identity theft, and one count of theft of government property. In an October 2007 plea hearing, Barnes admitted to having used her position as a Girl Scout leader to obtain personal history information from the members of her troop. Barnes created a fraudulent "Girl Scout Medical Release" form in order to get personal information from her scouts, including SSNs. Barnes used the children's SSNs to file electronic income tax returns with the IRS, submitting false information regarding income and employment.

▶ *Evaluate Monetary Thresholds for Prosecution*

The Task Force recommended that U.S. Attorneys' Offices consider lowering current monetary thresholds for initiating identity theft cases, recognizing that monetary loss may not always adequately reflect the harm caused by thieves and that the aggravated identity theft statute allows the government to obtain significant sentences even where monetary losses cannot be precisely calculated. Accordingly, most U.S. Attorneys' Offices have re-evaluated the monetary threshold for identity theft cases in the last year. The districts vary greatly in size, population, crime demographics, and the level of state and local resources, and so their monetary thresholds vary accordingly. The vast majority of districts do not have a bright-line monetary threshold for identity theft cases, and some districts employ no monetary threshold at all. The intent of all districts is to prosecute as many identity theft cases as resources allow and to give special consideration to prosecuting aggravated identity theft cases.

▶ *Encourage State Prosecution of Identity Theft*

The Task Force recommended that DOJ encourage state prosecutions of identity theft. Most U.S. Attorney's Offices have built strong channels of communication with their respective state prosecutors and investigators who work on identity theft crimes. These relationships are intended to ensure efficient use of resources and the most effective prosecutorial outcomes. Depending on the circumstances, federal investigators may support state prosecutions, or state investigators may contribute to federal prosecutions.[73]

Over the past year, DOJ has increased its efforts to work with state prosecutors. For example, the U.S. Attorney's Office for the Western District of Washington has developed strong working relationships with the state prosecutors who work in specialized identity theft units in that district. These state prosecutors often will ask the federal identity theft coordinator to consider seeking a federal indictment against state defendants who refuse to accept a state plea offer. If the state case merits potential federal prosecution, the AUSA will send a letter to the state prosecutor outlining the potential federal charges and penalties against the defendant. This letter authorizes the state prosecutor to instruct defense counsel that, unless the defendant accepts the state's plea offer, the U.S. Attorney's Office will pursue charges.

The Internet Crime Complaint Center (IC3) provides case referrals to state and local law enforcement agencies. IC3 is currently in the planning stages of a technological upgrade that will enable state law enforcement agencies to access information directly from the IC3 database and to request analytical assistance from IC3 on data related to crimes. For more information about IC3, *see* Recommendation 17, pp. 29–31.

The FTC's Identity Theft Data Clearinghouse also supports state and local prosecutors and investigators. Victim complaint data, litigation resources, and

automatic query functions enable law enforcement agencies and prosecutors across the country to gather information about suspects, contact victims, and determine whether other agencies are involved in an investigation. For more information about the FTC's Identity Theft Data Clearinghouse, *see* Recommendation 17, pp. 29–31.

▶ *Create Working Groups and Task Forces*

The Task Force recommended that U.S. Attorney's Offices and investigative agencies make increased use of interagency working groups and task forces devoted to identity theft and, where funds for task forces are not available, consider forming working groups with non-dedicated personnel.

Most U.S. Attorneys' Offices now participate in multi-agency task forces or working groups that address local and regional identity theft issues. Formal working groups typically involve federal and state law enforcement investigators, prosecutors, and financial institution fraud investigators. Typically, these working groups meet regularly for training, case review, and coordination to avoid redundant or overlapping efforts. In addition to DOJ, the U.S. Postal Inspection Service and the U.S. Secret Service are active participants in these groups. These groups link federal, state, and local law enforcement officers for investigations of all types of identity theft crimes.

Many districts have hosted identity theft seminars for federal, state, and local law enforcement officers and prosecutors. These seminars are usually sponsored by the identity theft working groups or task forces, or one of the members thereof. For example, the U.S. Attorney's Office for the District of Delaware recently participated in a successful identity theft summit sponsored by the Delaware Attorney General's Office. Other districts have plans to host such events.

In fiscal year 2008, the U.S. Postal Inspection Service has increased the number of financial crimes task forces that it leads throughout the country from 14 to 29. These task forces focus on identity theft crimes and are comprised of local, state, and federal law enforcement agencies.

An 18-month investigation of a large identity theft ring by a joint task force of federal and state law enforcement recently resulted in lengthy prison sentences for the ring leader and his co-conspirators. Charles W. Griffin of Federal Way, Washington, was sentenced in December 2007 to more than seven years in prison, five years of supervised release, and $241,492 in restitution for leading a conspiracy to commit identity theft, bank fraud, and one count of aggravated identity theft. This scheme recruited insiders at a mortgage company and escrow firm to obtain clients' personal and financial information. They used this information to make counterfeit drivers' licenses, take over bank accounts and drain them, open credit accounts in victims' names, and run up thousands of dollars in bills. In total, the conspirators obtained over $335,000 in goods. The primary "runner" who used the stolen identities, Elizabeth Angous, was sentenced to nearly eight years in prison for bank fraud, wire fraud, Social Security fraud, credit card fraud, and aggravated identity theft.

▶ RECOMMENDATION 26: CONDUCT TARGETED ENFORCEMENT INITIATIVES

The Task Force recommended several targeted enforcement initiatives directed at various aspects of identity theft.

▶ *Unfair or Deceptive Means To Make SSNs Available for Sale*

DOJ and various federal investigative agencies have investigated and prosecuted a number of cases involving the illegal compromise and sale of SSNs and other personal and financial data. *See supra* Recommendation 25, pp. 37-41.

In addition, the SSA OIG continues to monitor the Internet for sites that provide services related to the purchase or sale of SSNs. When it finds such sites, the SSA OIG reviews them for potential criminal and civil violations.

▶ *Identity Theft Related to the Health Care System*

The Department of Health and Human Services, Office of Inspector General, Office of Investigations (HHS-OIG) has investigated several cases of identity theft relating to Medicare and Medicaid fraud and, while no evidence of wide-scale identity theft of Medicare beneficiaries caused by the use of SSNs was found in the Medicare program, these cases fell into two categories. In some of these cases, the victim of identity theft was a recipient of Medicare or Medicaid services, and the thief used the victim's identity to fraudulently obtain benefits for which the thief otherwise did not qualify. In other cases, identity thieves stole physicians' identities in order to fraudulently bill Medicare and Medicaid for services not provided.

In one recent prosecution, the U.S. Attorney for the District of Utah obtained convictions against Ruben Curiel, George Davila, Jr., and Mary Davila, who were sentenced to prison terms ranging from 12 to 42 months and ordered to pay restitution and fines for aggravated identity theft, health care fraud, and other violations. These defendants, along with two other co-defendants, were ordered to pay a total of $25,601 in restitution to Medicaid and private insurers. The defendants had obtained physicians' Drug Enforcement Administration (DEA) numbers in order to obtain fraudulent prescriptions without the physicians' knowledge or consent. Many of the prescriptions were billed to Medicaid and private insurance. The investigation was conducted by the HHS-OIG and the Utah Medicaid Fraud Control Unit.

In another recent example, Laurie Gilliland was sentenced to 44 months in prison and five years of probation and ordered to pay restitution in the amount of $13,632 and a $500 special assessment for aggravated identity theft, among other offenses. She had assumed the identity of a family friend by obtaining a duplicate copy of her friend's Social Security card. Gilliland used the victim's identity to obtain medical treatment.

In the past year, DOJ formed task forces based in the Southern District of Florida and the Central District of California to prosecute significant health care fraud cases. These cases often include identity theft as part of the fraudulent operations.

▶ *Identity Theft by Illegal Aliens*

The Task Force recommended that DHS conduct enforcement initiatives against illegal aliens who use stolen identities to enter or stay in the United States and those who assist them. DHS targets this type of identity theft through its Immigration and Customs Enforcement (ICE) Identity and Ben-

efit Fraud Program and its Worksite Enforcement Program. Over the past year, these programs have increased efforts to reduce identity theft by illegal aliens.

Identity and Benefit Fraud Program. ICE's Identity and Benefit Fraud Program focuses on identity fraud and the manufacturing, counterfeiting, alteration, and use of identity documents to circumvent immigration laws and commit other criminal activity. ICE investigations have targeted individuals and organizations that sell and use unlawfully obtained identity documents and data to provide aliens with identities and illegal means to enter, reside, work, and remain in the United States.

ICE conducts some of its most effective work in this area through task forces that partner with other federal and local law enforcement agencies. On April 25, 2007, ICE launched an additional six Document and Benefit Fraud Task Forces (DBFTFs), bringing the total nationwide to seventeen. The DBFTFs target the criminal organizations that facilitate the unlawful entry, residence, and employment of illegal aliens.

Worksite Enforcement Program. ICE's Worksite Enforcement Program combats illegal employment by targeting egregious abuses by employers who hire illegal aliens. These violations range from actively recruiting undocumented workers in their countries of origin to ignoring or encouraging blatant fraud and identity theft by their workforce. To identify potential targets for investigation, ICE frequently works with other law enforcement agencies such as the FTC, the SSA OIG, and state labor agencies. A few examples of ICE's recent Worksite Enforcement Program efforts include the following:

- In May 2007, ICE agents administratively arrested 136 undocumented workers at George's Processing, a poultry processing plant in Barry County, Missouri. Through the use of undercover contacts, interviews of apprehended aliens, and analysis of wage reports, ICE obtained evidence that some managers and supervisors had direct knowledge that many of their employees were undocumented aliens and encouraged them to engage in identity theft to evade the Form I-9 Employee Eligibility Verification requirements.
- In July 2007, ICE agents arrested 30 Swift & Company employees, including a Swift Human Resource employee and a union official, on identity theft-related charges. This sweep followed almost 300 arrests of employees at Swift in December 2006 for identity theft and other crimes.
- In August 2007, ICE agents arrested 24 undocumented workers at a Smithfield Processing Plant in Tar Heel, North Carolina who were charged later with identity theft, reentry after deportation, and fraud and misuse of visas.

- In May 2008, ICE agents detained 389 people at the Agriprocessors, Inc. plant in Postville, Iowa, on suspicion of immigration violations. Of those, 305 were charged criminally for identity theft and other crimes. At least 230 defendants pleaded guilty to using false identification to obtain employment after admitting using an actual person's identity and were sentenced to five months' incarceration and three years' supervision.

In addition to these immigration programs and initiatives, DHS has numerous screening and credentialing programs, including REAL ID, E-Verify, and the Western Hemisphere Travel Initiative (WHTI). These programs should reduce the likelihood that an individual could fraudulently obtain identity documents in another's name. They target identity theft through enhanced authentication of individuals seeking driver's licenses and travel documents, and the use of databases to screen individuals seeking employment. Although these initiatives are helpful in combating illegal immigration, their benefits extend beyond that context.

REAL ID. REAL ID will establish minimum standards for state issued driver's licenses and identification cards, including electronic verification of the identity and lawful status of an individual before a card can be issued; and security requirements for card production facilities and the protection of personal data. As a result, REAL ID will strengthen initial authentication standards, ensuring that identity documents are issued only to the appropriate individuals. Because driver's licenses are used to identify individuals in a wide range of settings (including air travel, financial transactions, and commerce), the strengthened authentication requirements contained in REAL ID have the potential to restrict the ability of identity thieves to obtain licenses in another's name.

Western Hemisphere Travel Initiative. WHTI is a joint plan by the DHS and Department of State to require all previously exempt travelers to present a passport or alternative document establishing identity and citizenship when entering the U.S. from within the Western Hemisphere. By limiting the number of documents accepted at the border, WHTI decreases opportunities for fraud. In addition, through WHTI, border officers will be able to electronically verify a document with its issuing agency. This further reduces the likelihood that an individual could enter the U.S. using a stolen identity.

E-verify. E-Verify is a system used to verify a new hire's identity and work authorization status against Social Security Administration and Department of Homeland Security records. It is widely used by Federal, State, and local government agencies, by Federal contractors, and by private businesses to verify the employment authorization of their new employees. By verifying the identity and work authorization documents each employee presents upon being hired as part of the form I-9 Employment Eligibility Verification process,

E-Verify prevents illegal aliens from utilizing fraudulent documents to gain employment.

RECOMMENDATION 27: REVIEW CIVIL MONETARY PENALTY PROGRAMS

The Task Force recommended that federal agencies review their civil monetary penalty programs to assess whether they adequately address identity theft.

The FTC has conducted such a review and concluded that it would benefit from having civil penalty authority in data security cases. Although the FTC, a civil enforcement agency, cannot enforce criminal identity theft laws, it can take law enforcement action against businesses that fail to implement reasonable safeguards to protect sensitive information from identity thieves. After reviewing its authority in the data security context, the Commission concluded that its traditional equitable remedies, including consumer restitution and disgorgement of ill-gotten gains, are inadequate. Restitution is often impracticable in these cases because consumers suffer injury that is either non-economic in nature or difficult to quantify. Likewise, disgorgement may be unavailable because the defendant generally has not profited directly from his unlawful acts. In order to obtain relief that can better protect consumers and more effectively deter unlawful conduct in this area, the Commission has asked Congress to provide civil penalty authority in data security cases.[74]

The Board, FDIC, OCC, OTS, and the National Credit Union Administration (NCUA) have concluded that their existing enforcement authority, which includes civil money penalty authority, enables them to take effective actions to address identity theft with respect to the institutions subject to their jurisdiction.

The SSA OIG enforces two civil monetary penalty statutes that address SSN misuse.[75] Pending legislative proposals would enhance SSA OIG's authority to impose civil monetary penalties for SSN misuse, including on the Internet.[76]

RECOMMENDATION 28: CLOSE THE GAPS IN FEDERAL CRIMINAL STATUTES USED TO PROSECUTE IDENTITY-THEFT-RELATED OFFENSES TO ENSURE INCREASED FEDERAL PROSECUTION OF THESE CRIMES

See supra Recommendation 14, p. 27.

RECOMMENDATION 29: ENSURE THAT AN IDENTITY THIEF'S SENTENCE CAN BE ENHANCED WHEN THE CRIMINAL CONDUCT AFFECTS MORE THAN ONE VICTIM

The Task Force recommended that the U.S. Sentencing Commission (Sentencing Commission) amend the definition of "victim" in section 2B1.1 of the U.S. Sentencing Guidelines to clarify that a victim need not have suffered an actual monetary loss to be considered a victim for sentencing purposes. Specifically, the Task Force recommended that a victim be defined as any person who sustained any monetary or non-monetary harm, including the theft of a means of identification, invasion of privacy, reputational damage, and inconvenience. This proposal also would allow enhancement of the defendant's sentence if the identity theft affected more than one victim. The Task Force forwarded this proposal in 2007 to the Sentencing Commission for consideration as part of its annual review of possible amendments to the U.S. Sentencing Guidelines.

RECOMMENDATION 30: ENHANCE TRAINING FOR LAW ENFORCEMENT OFFICERS AND PROSECUTORS

Because training can be the key to effective investigations and prosecutions, the Task Force recommended that member agencies expand their law enforcement and prosecutor training programs in the following ways.

Develop Course at the National Advocacy Center Focused Solely on Investigation and Prosecution of Identity Theft

DOJ, the FTC, and other agencies have taken significant steps to provide all levels of law enforcement with appropriate training on identity theft. Task Force member agencies have led two seminars at DOJ's National Advocacy Center dedicated exclusively to identity theft investigation and prosecution by federal authorities, the more recent of which was held in February 2008.

The March 2008 issue of *USA Bulletin*, a periodic publication from the Executive Office for United States Attorneys, provided extensive information by seminar instructors for prosecutors and investigators on identity theft. Articles discuss applicable statutes and charging decisions, the use of Social Security numbers in identity theft, and various localized approaches to tackling identity theft. *See www.usdoj.gov/usao/reading_room/foiamanuals.html.*

Increase Number of Regional Identity Theft Seminars

DOJ, the FTC, the U.S. Secret Service, the U.S. Postal Inspection Service, the FBI, and the American Association of Motor Vehicle Administrators jointly have been sponsoring regional training seminars on identity theft for state and local law enforcement officers since May 2002. Since the release of the Strategic Plan, two seminars were held in the Chicago area in September 2007, two seminars were held in North and South Carolina in January 2008, one was held in Minneapolis in April 2008, one was held in Alabama in July 2008, and one was held in Atlanta in July 2008. In total, over 900 law enforcement officers from over 250 agencies attended these seminars. Additional seminars are scheduled for the remainder of 2008.

Increase Resources for Law Enforcement Available on the Internet

The Task Force agencies also have been increasing online resources about identity theft for law enforcement agencies. For example, since the issuance of the Strategic Plan, DOJ has increased the amount of information available to the public and law enforcement through the Internet as well as through internal networks for sensitive information relating to investigations and prosecutions. In addition to the resources available through *www.idtheft.gov*, DOJ has made resources available through *www.cops.usdoj.gov/ric* and *www.cybercrime.gov*, including the 2007 manual "Prosecuting Computer Crimes," which covers issues relating to investigating and prosecuting data breaches and related computer frauds. Other materials available include manuals and guidance on collecting electronic evidence, which is critical for effectively prosecuting identity theft. DOJ also has made sample indictments and other relevant information available to investigators and prosecutors at all levels of government.

Review Curricula To Enhance Basic and Advanced Training on Identity Theft

The FBI, the U.S. Secret Service, the U.S. Postal Inspection Service, and the Federal Law Enforcement Training Center have reviewed their curricula and have ensured that they are providing suitable basic and advanced training on identity theft. The U.S. Postal Inspection Service held a pilot training course for Postal Inspectors in July 2007 and held a training course in March 2008. The U.S. Postal Inspection Service will provide additional courses in 2009.

RECOMMENDATION 31: ENHANCE THE GATHERING OF STATISTICAL DATA MEASURING THE CRIMINAL JUSTICE SYSTEM'S RESPONSE TO IDENTITY THEFT

The Task Force recognized that, in order to understand and properly respond to identity theft, the federal government needs access to comprehensive statistical data about the crime and the success of law enforcement's efforts to combat it. This recommendation was designed to encourage the government to collect additional data from victims, law enforcement agencies, and courts to provide a more complete picture of the crime and its impact.

Gather and Analyze Statistically Reliable Data from Identity Theft Victims

The Task Force recommended that its members continue to gather and analyze statistically reliable data from identity theft victims. In November 2007, the FTC released the results of its 2006 identity theft survey.[77] This survey of almost 5,000 individuals found that approximately 8.3 million adults, or 3.7% of all American adults, became victims of identity theft in 2005. Of the victims, 3.2 million, or 1.4% of all adults, experienced only the misuse of

their existing credit card accounts, 3.3 million, or 1.5%, experienced misuse of non-credit card accounts, and 1.8 million, or 0.8%, found that new accounts were opened or other frauds were committed using their personal identifying information.

The survey consistently found greater costs—such as thieves obtaining more goods and services and victims spending more time and money recovering—in cases where the thief opened new accounts rather than only hijacking existing accounts. For example, where the theft was limited to the misuse of existing accounts, the median value of goods and services obtained by the thieves was less than $500. In cases where the thieves opened new accounts or committed other frauds, the median value of goods and services they obtained was $1,300.

In order to include more consumers in future surveys, and develop even more meaningful data, the FTC is working with DOJ's Bureau of Justice Statistics (BJS) to include additional questions on identity theft in the ongoing National Crime Victimization Survey (NCVS), which is described below. An identity theft supplement will be included with the NCVS in the first six months of 2008.

▶ *Expand Scope of the National Crime Victimization Survey and Conduct Targeted Surveys*

The Task Force recommended that the annual NCVS be expanded to collect greater information about identity theft victims and that BJS, the entity primarily charged with collecting statistical data for DOJ, continue to conduct targeted surveys related to identity theft. Below is a description of BJS' current data collections related to identity theft:

National Crime Victimization Survey—Identity Theft Supplement. BJS has added a supplement devoted exclusively to identity theft to the NCVS from January through June 2008. This collection will enable BJS to estimate the types of identity theft victimization as well as gather data on financial loss, emotional impact, and law enforcement response. Data from this collection will be available in 2009.

State Court Processing Statistics. The current State Court Processing Statistics data collection will attempt to identify the number of felony defendants charged with identity theft in the nation's 75 most populous counties. It will have pretrial release, adjudication, and sentencing information on these defendants. These data should be delivered in the summer of 2008, and information from this series will be published in 2009.

National Census of State Court Prosecutors. Five questions about identity theft were added to this data collection to measure the types of investigations and charges filed by state prosecutors. The data are expected in early 2009.

Census of Public Defender Offices. The Census will identify the types of identity theft cases being handled by public defender offices nationwide. This data will enable BJS to provide information on the number of offices providing representation to indigent defendants accused of credit card fraud, internet identity theft, embezzlement, mail fraud, bank fraud, or use of stolen checks. Data from this collection will be available in 2009.

▶ *Review Sentencing Commission Data*

The Task Force recommended that DOJ and the FTC systematically review and analyze Sentencing Commission identity theft-related case files every two to four years, and begin that work in the third quarter of 2007. Both DOJ and the FTC have begun this review and are considering review of possible additional material.

▶ *Track Prosecutions of Identity Theft and the Amount of Resources Spent*

The Task Force recommended that DOJ continue to track prosecutions of identity theft and federal resources spent on such cases. The U.S. Attorneys' Case Management System tracks district and nationwide identity theft statistics. Employees from each U.S. Attorney's Office enter data into the system per relevant statute, 18 U.S.C. §§ 1028 and 1028A. Identity theft statistics are tracked, analyzed, and extracted by the data analysis team of the Executive Office for U.S. Attorneys and are loaded onto the internal USAnet website. In 2007, identity theft was added as a category for tracking work hours. In fiscal year 2007, 25.68 attorney work years were devoted to identity theft prosecution nationwide.

During fiscal year 2007, 2,470 defendants were charged federally with identity theft under either 18 U.S.C. §§ 1028 or 1028A. During the same year, 1,943 convictions were obtained under those statutes, and 95.39% of the cases resolved resulted in a conviction.

Conclusion

The battle against identity theft is a shared responsibility. Consumers, businesses, and other organizations that collect consumer data; information technology and software providers that supply anti-fraud solutions; and federal, state, and local governments are all impacted by identity theft and have roles to play in the fight against it.

What makes identity theft especially challenging is its dynamic and rapidly-changing nature. The profiles, purposes, and methods of the perpetrators are continually changing. Identity theft today can be the product of organized crime rings here and abroad using increasingly sophisticated technologies, such as installing malicious software, phishing, spoofing, and database hacking, to tap into repositories of consumer data. Increasingly, criminals combine these techniques for better effect, many of which are facilitated by commercially available tools. At the same time, the more traditional "low tech" methods of stealing identities—insider breaches, dumpster diving, garden variety purse snatching, and the like—continue.

The fight against identity theft is an "end to end" challenge in which the security risks and responsibilities are spread from consumers, to enterprises, to information technology and telecommunication vendors, software providers, and others who facilitate the collection, use, maintenance, and eventual destruction of personal information. Newer areas of identity theft are growing fast, as thieves steal data in order to commit medical, immigration, employment, and mortgage fraud, for example. What identity theft will look like ten years from now is impossible to predict.

In April 2007, the Task Force released a plan for attacking identity theft that relies on the contributions of all stakeholders, working in cooperation. The Strategic Plan recommends the use of all available tools, from enhanced consumer and business education, to better data security and consumer authentication, to expanded resources for victim recovery, to increased training and support for our foreign law enforcement partners, to more certain and stronger punishment for perpetrators.

Over the past year or so, the Task Force members have worked to implement the recommendations of the Strategic Plan. Much of this work has been completed; some is ongoing. Many in the private and not-for-profit sectors also have taken important steps to reduce the incidence of identity theft. The fight against identity theft will not end when we have implemented the 31 recommendations in the Plan, however. Identity theft must be treated aggressively, yet with the recognition that it is an ongoing and evolving problem, that there is no "silver bullet" that will end it, and that its perpetrators will be ever more creative. Government and the private sector, working together with consumers, must remain vigilant, adaptable, and nimble as new generations of identity thieves and techniques develop over the coming years.

Appendix

Below are examples of Task Force member agency initiatives to reduce the unnecessary collection and use of SSNs.

- The SSA has reviewed the use of SSNs on its internal human resources forms and has removed them almost entirely. The SSA's Office of General Counsel also has made efforts to ensure that no SSNs are included in any litigation briefs or Freedom of Information Act-related correspondence.
- The Department of Defense (DOD) has developed policy for its internal use of SSNs and has issued a plan to reduce that use, including the removal of the SSN from Military ID cards.
- As of January 2008, the IRS has been redacting taxpayer SSNs to the last four digits on all federal tax lien documents filed in public records and issued to taxpayers and their representatives. The IRS currently is assessing the redaction of SSNs on other types of documents as well.
- The federal depository institution regulatory agencies have surveyed their internal records and taken steps to minimize unnecessary use of SSNs. For example, the FDIC removed SSNs from seven of its systems, masked SSNs in one system, and significantly reduced the number of users with access in four other systems. The Board, OTS, and OCC have reduced the use of SSNs in connection with their personnel-related systems, to the extent possible. The NCUA has eliminated the use of SSNs on all internal NCUA systems.
- DHS has undertaken a full review of its use of SSNs. DHS issued policy guidance to all personnel in June 2007 that reiterated previous federal guidance on the use of SSNs and established a process to review existing and new uses of SSNs. In accordance with this guidance, all systems that use or collect SSNs now submit to the DHS Privacy Office a Privacy Threshold Analysis (PTA) that specifically identifies and analyzes the propriety of SSN use by that system. As a result of this process, DHS has eliminated the use or collection of SSNs in five systems and has confirmed the necessity and that appropriate safeguards exist for the majority of its remaining systems that use or collect SSNs.
- The VA has taken many steps in the past year to reduce unnecessary uses of SSNs and strengthen its data security program generally. For example, it has truncated the SSN field of many electronic data interchange transactions to the last four digits of the SSN. It also has installed a filter on all VA electronic mail gateways to scan outgoing email for patterns resembling SSNs and to block all email containing such a pattern. In addition, it has developed management, operational, and technical controls for data security to be instituted by all VA offices. Finally, the VA has issued detailed guidance on protecting portable storage and communications devices.

Endnotes

1. Executive Order 13402, May 10, 2006.

2. One recent survey of over 2,000 Americans by the University of Southern California's Center for the Digital Future, for example, found that 61 percent of the population are very or extremely concerned about the privacy of their personal information when shopping online (up from 46 percent the year before). The Center for the Digital Future at the University of Southern California Annenberg School, Surveying the Digital Future (2007), available at ***www.digitalcenter.org/pdf/2008-Digital-Future-Report-Final-Release.pdf***. A contemporaneous survey found that 62 percent of consumers were less likely to shop at a retailer that had announced a data breach, while 47 percent stated that recent breaches make them feel less comfortable using credit card data for online shopping. Utimaco Safeware Inc., Utimaco Survey Reveals Holiday Shoppers are Less Likely to Patronize Breached Retailers (Dec. 18, 2007), available at ***www.americas.utimaco.com/news/stories/2007/Holiday-Survey-Results.html***.

3. *See* Federal Trade Commission, "Protecting Personal Information: A Guide For Business" (2007), available at ***www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf***.

4. For example, the Internal Revenue Service (IRS) has nearly completed its phase-out of SSNs for identifying its 100,000 employees and contractors, except where required for income reporting, background checks, and matching with employment records for external entities. Instead, IRS now uses a five-character Standard Employee Identifier. Similarly, the Department of Veterans Affairs (VA) is developing a plan to move away from the SSN as a primary identifier of veterans and will begin in early 2009 to implement an interim employee identifier that is similar to OPM's proposed UEID. The U.S. Postal Service has implemented its own employee identifier and is working to eliminate the use of SSNs and other sensitive data elements.

5. *See* Memorandum from Linda M. Springer, Director, Office of Personnel Management, to Chief Human Capital Officers Regarding Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft, June 18, 2007, available at ***www.chcoc.gov/transmittal_detail.cfm?ID=847***.

6. *See*, e.g., Social Security Administration Office of the Inspector General Reports: "Federal Agencies' Controls over the Access, Disclosure, and Use of Social Security Numbers by External Entities," Mar. 11, 2003, available at ***www.ssa.gov/oig/ADOBEPDF/A-08-03-13050.pdf***; "Removing Social Security Numbers from Medicare Cards," May 2, 2008, available at ***www.ssa.gov/oig/ADOBEPDF/A-08-08-18026.pdf***; "Universities' Use of Social Security Numbers as Student Identifiers in Region IV," Dec. 9, 2004, available at ***www.ssa.gov/oig/ADOBEPDF/A-08-05-15034.pdf***; "Hospitals' Use and Protection of Social Security Numbers," Jan. 27, 2006, available at ***www.ssa.gov/oig/ADOBEPDF/A-08-06-16056.pdf***; "Prisoners' Access to Social Security Numbers," Aug. 23, 2006, available at ***www.ssa.gov/oig/ADOBEPDF/A-08-06-16082.pdf***; and "State and Local Governments' Collection and Use of Social Security Numbers," Sept. 10, 2007, available at ***www.ssa.gov/oig/ADOBEPDF/A-08-07-17086.pdf***.

7. *See* Memorandum from Clay Johnson III, Deputy Director for Management, Office of Management and Budget, to the Heads of Executive Departments and Agencies Regarding Safeguarding Against and Responding to the Breach of Personally Identifiable Information (M-07-16), May 22, 2007, available at ***www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf***.

8. *See* Memorandum from Clay Johnson III, Deputy Director for Management, Office of Management and Budget, to the Heads of Executive Departments and Agencies Regarding FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (M-08-21), July 14, 2008, available at ***www.whitehouse.gov/omb/memoranda/fy2008/m08-21.pdf***.

9. *See* Testimony of the Federal Trade Commission Before the Ohio Privacy and Public Records Access Study Committee of the Ohio Senate and House of Representatives, "Public Entities, Personal Information, and Identity Theft" (May 31, 2007), available at ***www.ftc.gov/os/2007/05/070531ohiotest.pdf***, *see* also Testimony of the Federal Trade Commission Before the Maryland Task Force to Study Identity Theft, "Combating Identity Theft: Implementing a Coordinated Plan" (Sept. 18, 2007), available at ***www.ftc.gov/os/2007/09/P075418idtheft.pdf***.

10. *See* National Conference of State Legislatures, Fall Forum 2007, Nov. 28, 2007, agenda available at ***www.ncsl.org/standcomm/sccomfc/CFIFallForum07Agenda.htm***.

11. *See* SSA OIG, "State and Local Governments' Collection and Use of Social Security Numbers," Sept. 10, 2007, available at ***www.ssa.gov/oig/ADOBEPDF/A-08-07-17086.pdf***.

12. IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities, available at ***www.irs.gov/pub/irs-pdf/p1075.pdf***.

13. *See* ***csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf***. This memorandum incorporates comments received during a public forum hosted on May 11, 2007 by DHS and OMB, as well as comments submitted through interagency review. In addition, the memorandum incorporates other resources, including the DHS interagency Critical Infrastructure Protection Cyber Policy Coordinating Committee Working Group's white paper titled "Network Architecture and Data Handling."

14. For example, the FTC's Chief Privacy Officer delivered presentations regarding effective data breach response at the Homeland Defense Journal's July 2007 training on "Strategies for Data Beach Prevention, Mitigation, and Notification," a November 2007 workshop entitled "Privacy Challenges in Government," and the 2007 Federal IT Summit, co-sponsored by the OMB's Office of Electronic Government and the Federal Chief Information Officers Council's IT Workforce Committee. In 2007, the FTC's Chief Privacy Officer also spoke to the Small Agency CIO Council about laptop security and creative ways to train federal employees on safeguarding portable IT devices.

15. For more information about the President's Management Agenda, *see* ***www.whitehouse.gov/results/agenda/index.html***.

16. *See* supra note 7.

17. *See* Section 208 of the E-Government Act. For more information about PIAs, *see* Memorandum from Joshua B. Bolton, Director, Office of Management and Budget, to the Heads of Executive Departments and Agencies Regarding Implementing the Privacy Provisions of the E-Government Act of 2002 (M-03-22), Sept. 23, 2003, available at ***www.whitehouse.gov/omb/memoranda/m03-22.html***.

18. *See* supra note 8.

19. *See* id.

20. *See* supra note 7.

21. *See* Memorandum from Clay Johnson III, Deputy Director for Management, Office of Management and Budget, to the Heads of Departments and Agencies Regarding Protection of Sensitive Agency Information (M-06-16), June 23, 2006, available at ***www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf***.

22. This also was one of the interim recommendations issued by the Task Force on September 19, 2006. *See* ***www.ftc.gov/opa/2006/09/idtheft.shtm***. The OMB guidance is reproduced in Appendix A of the Identity Theft Task Force's Strategic Plan (Apr. 2007), available at ***www.idtheft.gov/reports/StrategicPlan.pdf.***

23. *See* supra note 7.

24. For example, the Privacy Act of 1974 requires federal agencies to establish rules of conduct for persons involved in the design, development, operation, and maintenance of any system of records, establish appropriate safeguards to ensure the security and confidentiality of such records, and maintain accurate information about such records. 5 U.S.C. § 552a(e).

25. *See* the Privacy Act of 1974, 5 U.S.C. 552a(b).

26. Department of Justice, AAG/A Order No. 001-2007, Privacy Act of 1974; Systems of Records, 72 FR 3410 (Jan. 25, 2007).

27. *See*, e.g., Notice of Amendment to System Name and Addition to Routine Uses, 73 FR 29181 (May 20, 2008) (VA); Notice to Amend All Privacy Act Systems of Records, 72 FR 31835 (June 8, 2007) (Department of Commerce); Notice of Routine Use, 72 FR 31835-01 (June 8, 2007) (FTC); Notice of New Routine Use, 72 FR 43296 (August 3, 2007) (Nuclear Regulatory Commission); Proposed Routine Use, 72 FR 44878 (August 9, 2007) (Peace Corps).

28. *See*, e.g., Testimony of Joel Winston Before the House Subcommittee on Crime, Terrorism, and Homeland Security, "Protecting Consumer Privacy and Combating Identity Theft" (Dec. 18, 2007), available at ***www.ftc.gov/os/testimony/P065404idtheft.pdf***.

29. *See* "FTC, IAPP, Northwestern University Law School to Co-host April 15 Workshop for Businesses on Best Practices for Protecting Personal Information and Securing Data" (Feb. 1, 2008), available at ***www.ftc.gov/opa/2008/02/data.shtm***.

30. *See* "FTC, California Office of Privacy Protection to Co-Host Workshop for Businesses on Best Practices for Protecting Personal Information and Securing Data," (July 22, 2008), available at ***www.ftc.gov/opa/2008/07/datasec.shtm***.

31. *See* FFIEC Information Technology Examination Handbook: Business Continuity Planning Booklet (Mar. 19, 2008), available at ***http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#bcp***.

32. *See* ***www.ftc.gov/bcp/conline/edcams/infosecurity/publish.html***.

33. *See* "FTC Reminds Businesses: Don't Print Full Credit and Debit Card Numbers on Customers' Purchase Receipts" (Dec. 14, 2007), available at ***www.ftc.gov/opa/2007/12/slip.shtm***.

34. *See* FDIC, FIL-32-2007, Supervisory Policy on Identity Theft (Apr. 11, 2007), available at ***www.fdic.gov/news/financial/2007/fil07032.html***.

35. *See* 12 CFR part 30, supp. A to app. B (OCC); 12 CFR part 208, supp. A to app. D-2 and part 225, supp. A to app. F (Federal Reserve); 12 CFR part 364, supp. A to app. B (FDIC); 12 CFR part 570, supp. A to app. B (OTS)Need cites. The Response Program Guidance interprets the agencies' Guidelines Establishing Information Security Standards. *See* 12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D-2 and part 225, app. F (Board); 12 CFR part 364, app. B (FDIC); 12 CFR part 570, app. B (OTS).

36. United States v. American United Mortgage Co., No. 07C 7664 (N.D. Ill.) (Stipulated Final Judgment and Order entered on Jan. 28, 2008) (alleged violations of the FTC's Disposal Rule where documents containing sensitive personal information were thrown in an unsecured dumpster), available at ***www.ftc.gov/os/caselist/0623103/index.shtm***; In the Matter of The TJX Companies, Inc., FTC File No. 072-3055 (Mar. 27, 2008) (Proposed Consent Order) (alleged failure by retailer to use reasonable security measures to prevent unauthorized access to personal information on its computer networks, resulting in a hacker obtaining tens of millions of credit and debit card numbers and making millions of dollars in unauthorized charges), available at ***www.ftc.gov/opa/2008/03/datasec.shtm***; In the Matter of Reed Elsevier Inc. and Seisint, Inc., FTC File No. 052-3094 (Mar. 27, 2008) (Proposed Consent Order) (alleged failure by data brokers to implement reasonable access controls for their databases containing sensitive consumer information, including by allowing users to select easy-to-guess credentials), available at ***www.ftc.gov/opa/2008/03/datasec.shtm***; In the Matter of Life is good, Inc., FTC Docket No. C-4218 (Apr. 16, 2008) (Final Consent Order) (alleged failure to protect credit card numbers from electronic attacks, contrary to company's representations about its information security practices), available at ***www.ftc.gov/opa/2008/04/ligfyi.shtm***; United States v. ValueClick, Inc., No. CV08-01711 (C.D. Cal.) (Stipulated Final Judgment and Order entered on Mar. 17, 2008) (defendants paid $2.9 million in civil penalties to settle charges that advertising claims and emails were deceptive and violated federal law, as well as charges that they failed to encrypt and secure sensitive customer information against electronic attacks, contrary to representations), available at ***www.ftc.gov/opa/2008/03/vc.shtm***; In the Matter of Goal Financial,

LLC, FTC Docket No. C-4216 (Apr. 9, 2008) (Final Consent Order) (alleged security failures that resulted in inadvertent transfer of 7,000 student loan application files to third parties), available at ***www.ftc.gov/os/caselist/0723013/index.shtm***.

37. *See* "Company Will Pay $50,000 Penalty for Tossing Consumers' Credit Report Information in Unsecured Dumpster" (Dec. 18, 2007), available at ***www.ftc.gov/opa/2007/12/aumort.shtm***.

38. The FTC was able to obtain a civil penalty in this case because the defendant allegedly violated the Disposal Rule under the FCRA, a statute that authorizes the agency to seek penalties. In data security cases that do not involve violations of the FCRA, but rather are brought under the FTC Act or the Gramm-Leach-Bliley Act, civil penalties are not available. The agency has urged Congress to provide civil penalty authority in data security cases. *See* Testimony of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on the Commission's Work to Protect Consumers and Promote Competition, and on a Bill to Reauthorize the Commission, (Apr. 8, 2008), available at ***www.ftc.gov/opa/2008/04/reauth.shtm***.

39. *See* SEC, Public Alert: Unregistered Soliciting Entities (PAUSE), available at ***www.sec.gov/investor/oiepauselist.htm***; SEC Press Release 2007-34, SEC Suspends Trading Of 35 Companies Touted In Spam Email Campaigns (Mar. 8, 2007), available at ***www.sec.gov/news/press/2007/2007-34.htm***.

40. *See* Symantec Internet Security Report, Trends for January–June 07, Volume XII, at 107 (Sept. 2007), eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf (last visited July 7, 2008) (stating that a 30 percent decrease in stock market spam "was triggered by actions taken by the U.S. Securities and Exchange Commission, which limited the profitability of this type of spam").

41. *See* SEC Press Release 2007-33, SEC Obtains Order Freezing $3 Million in Proceeds of Suspected Foreign-Based Account Intrusion Scheme (Mar. 7, 2007), available at ***www.sec.gov/news/press/2007/2007-33.htm***.

42. *See* SEC Press Release 2007-40, SEC and U.S. Attorney Charge Three Offshore Hackers with Hijacking Online Brokerage Accounts, Manipulating Market (Mar. 12, 2007), available at ***www.sec.gov/news/press/2007/2007-40.htm***.

43. *See* "To Buy or Not to Buy: Identity Theft Spawns New Products and Services To Help Minimize Risk" (Nov. 2007), available at ***www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt05.shtm***.

44. *See*, e.g., ***www.treas.gov/offices/domestic-finance/financial-institution/cip/identity-theft.shtml*** (Treasury); ***www.ssa.gov/pubs/idtheft.htm*** (SSA); ***www.usps.com/postalinspectors/idthft_ncpw.htm*** (U.S. Postal Inspection Service).

45. *See* ***www.secretservice.gov/faq.shtml#faq12***.

46. The SSA publication, "Identity Theft and Your Social Security Number," is also available at ***www.socialsecurity.gov/pubs/10064.html***.

47. *See* ***www.federalreserveconsumerhelp.gov*** (Board); ***www.helpwithmybank.gov*** (OCC).

48. *See* ***www.ots.treas.gov***.

49. *See* "Don't Be an Online Victim: How to Guard Against Internet Thieves and Electronic Scams," available at ***www.fdic.gov/consumers/consumer/guard/***.

50. *See* ***www.sec.gov/investor/pubs/phishing.htm***.

51. In addition, the FTC's AvoID Theft Consumer Education Kit also can be ordered for free at ***www.ftc.gov/bulkorder.***

52. Deployments away from usual duty stations can make military personnel more vulnerable to identity theft, because it can be more difficult for them to monitor their mail and credit reports. For this reason, Congress amended the Fair Credit Reporting Act in 2003 to enable active duty military personnel to place an active duty alert in their credit files. Active duty alerts are designed to minimize the risk of identity theft by requiring businesses to verify the identity of active duty military personnel before issuing credit to them. *See* 15 U.S.C. § 1681c-1; *see also* FTC, "'Active Duty' Alerts Help Protect Military Personnel from Identity Theft," available at ***http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt147.shtm***.

53. *See* ***www.onguardonline.gov/idtheft.html***.

54. *See* ***www.idtheft.gov/takeaction.html***.

55. *See* ***www.ftc.gov/bcp/workshops/proofpositive/index.shtml***.

56. *See* Recommendation 11, p. 23.

57. The commenters included representatives of the financial services industry, law enforcement agencies, consumer reporting companies, academics, and consumer advocates. The comments are available at ***www.ftc.gov/os/comments/ssnprivatesector/index.shtm***.

58. *See* "FTC Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers" (Nov. 2007), available at ***www.ftc.gov/bcp/workshops/ssn/staffsummary.pdf***.

59. *See* ***www.ftc.gov/bcp/workshops/ssn/index.shtml***.

60. Criminal Justice, "Identity Theft Victim Recovery Starts with Local Law Enforcement," December 2007.

61. *See* ***www.idtheft.gov/takeaction.html***; ***www.ftc.gov/bcp/edu/microsites/idtheft/consumers/rights.html***.

62. *See* ***www.ovcttac.org/calendar***.

63. *See* Identity Theft Enforcement and Restitution Act of 2007, S. 2168; Identity Theft Enforcement and Restitution Act of 2007, H.R. 6060.

64. On July 30, 2008, the Senate passed H.R. 5938, which included the Identity

Theft Enforcement and Restitution Act of 2008.

65. *See* FTC, "Identity Theft Victims' Statement of Rights," available at ***www.idtheft.gov/takeaction.html*** and ***www.ftc.gov/bcp/edu/microsites/idtheft/consumers/rights.html***.

66. *See* FTC Staff *See*ks Comments on Credit Freezes: Impact and Effectiveness (Jan. 10, 2008), available at ***www.ftc.gov/opa/2008/01/freeze.shtm***.

67. *See* U.S. Attorney's Office for the Eastern District of Pennsylvania, Press Release (July 10, 2008), available at ***www.usdoj.gov/usao/pae/News/Pr/2008/jul/niclerelease.pdf***.

68. Criminal Justice, "Identity Theft Victim Recovery Starts with Local Law Enforcement," Dec. 2007.

69. *See* "Getting Information from Businesses that Dealt with the Identity Thief," available at ***www.ftc.gov/bcp/edu/microsites/idtheft/consumers/modelletter.html***; "Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Thief," available at ***www.ftc.gov/bcp/edu/pubs/business/idtheft/bus66.pdf***.

70. The Subgroup is now gathering information about identity theft activities and legal measures from the G8 Member States. It will develop written guidance on essential elements of legislation needed to criminalize the acquisition, transfer, use, and possession of false identification documents and false identifying information, as well as the unauthorized acquisition, transfer, use, and possession of other natural persons' identification documents and identifying information.

71. Reshipping schemes are fraud schemes in which a criminal fraudulently orders high-value goods from merchants (typically with stolen or fraudulently obtained payment cards) and, to disguise the fact that the goods are intended to be shipped to a foreign country, arranges for initial delivery of the goods to a domestic address. Under the direction of the criminal, a person at that address then receives the goods and repackages and reships them to a foreign destination.

72. For example, the U.S. Attorney for the Eastern District of Pennsylvania has a regional identity theft working group comprised of law enforcement officers from local, state, and federal agencies. *See* ***www.usdoj.gov/usao/pae/Documents/identitytheft.htm***.

73. Federal prosecutors reach out to their state and local partners in a variety of ways. For example, the U.S. Attorney's Office for the Eastern District of Pennsylvania cross-designated an Assistant District Attorney at the Philadelphia District Attorney's Office as a Special Assistant United States Attorney (SAUSA). This SAUSA brought valuable state resources and local investigative relationships to the U.S. Attorney's Office in a recent and successful federal prosecution of a large identity theft ring.

74. *See*, e.g., Testimony of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on the Commission's Work to Protect Consumers and Promote Competition, and on a Bill to Reauthorize the Commission, (Apr. 8, 2008), available at ***www.ftc.gov/opa/2008/04/reauth.shtm***.

75. *See* Sections 1129 and 1140 of the Social Security Act, 42 U.S.C. §§ 1320a-8, 1320b-10.

76. *See* S. 238, Section 8, Social Security Number Misuse Prevention Act, available at ***www.frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s238is.txt.pdf***; H.R. 5234, Section 8, Social Security Number Misuse Prevention Act,available at ***www.frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h5234ih.txt.pdf***; H.R. 3046, Section 10, Social Security Number Privacy and Identity Theft Prevention Act of 2007, available at ***www.frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h3046rh.txt.pdf***.

77. 2006 Identity Theft Survey Report (Nov. 2007), available at ***www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf***.

Glossary of Acronyms

ABA—American Bar Association

AUSA—Assistant United States Attorney

BJS—Bureau of Justice Statistics (DOJ)

CDFO—Commercially-developed credit freeze option

CIO—Chief Information Officer

CIRFU—Cyber Initiative Resource Fusion Unit (FBI)

CMS—Centers for Medicare and Medicaid Services (HHS)

CRA—Consumer reporting agency

DBFTF—Document and Benefit Fraud Task Force

DEA—Drug Enforcement Agency

DHS—Department of Homeland Security

DOD—Department of Defense

DOJ—U.S. Department of Justice

FACT Act—Fair and Accurate Credit Transactions Act of 2003

FBI—Federal Bureau of Investigation

FCRA—Fair Credit Reporting Act

FDIC—Federal Deposit Insurance Corporation

FFIEC—Federal Financial Institutions Examination Council

FIMSI—Financial Industry Mail Security Initiative

FISMA—Federal Information Security Management Act

FTC—Federal Trade Commission

GAO—Government Accountability Office

GLB Act—Gramm-Leach-Bliley Act

IACP—International Association of Chiefs of Police

IAFCI—International Association of Financial Crime Investigators

IAPP—International Association of Privacy Professionals

IC3—Internet Crime Complaint Center

ICE—Immigration and Customs Enforcement (DHS)

IG—Inspector General

ILEA—International Law Enforcement Academy

IRPAC—Information Reporting Program Advisory Committee

IRS—Internal Revenue Service

ISI—Intelligence Sharing Initiative

IT—Information technology

MAGLOCLEN—Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network

NCFTA—National Cyber-Forensics and Training Alliance

NCIC—National Crime Information Center (FBI)

NCIJTF—National Cyber Investigative Joint Task Force

NCLR—National Council of La Raza

NCUA—National Credit Union Administration

NCVS—National Crime Victimization Survey

NICLE Network—National Identity Crimes Law Enforcement Network

OCC—Office of the Comptroller of the Currency

OMB—Office of Management and Budget

OPM—Office of Personnel Management

OTS—Office of Thrift Supervision

OVC—Office for Victims of Crime (DOJ)

PIA—Privacy Impact Assessment

PII—Personally identifiable information

PTA—Privacy Threshold Analysis

RITNET—Regional Identity Theft Network

SAUSA—Special Assistant United States Attorney

SEC—Securities and Exchange Commission

SSA—Social Security Administration

SSA OIG—Social Security Administration Office of the Inspector General

SSN—Social Security number

UEID CONOP—Unique Employee Identifier Concept of Operation

VA—Department of Veterans Affairs

VOCA—Victims of Crime Act